Crypto-Current

Nick Land

Contents:

Foreword	v
Chapter-1: Introduction	1
Chapter-2: Cryptocurrency as Critique	12
Chapter-3: Bitcoin and its Doubles	51
Chapter-4: State of Play	78
Chapter-5: Cash Machines	122
Chapter-6: The Open Secret	
Appendix-1: The 2008 Bitcoin Paper	
Appendix-2: Techonomics and Diagonal Method	
Appendix-3: Cryptocurrency and World Order	
Bitcoin Time-Line	
Coins	
Organizations	
People	
Websites	
Glossary	
Notes	
References	
URLs	

There is a sort of vast cycle of flows of production and chains of inscription, and a lesser cycle, between the stocks of filiation that connect or encaste the flows, and the blocks of alliance that cause the chains to flow.

– Gilles Deleuze and Félix Guattari[1]

Everybody needs money. That's why they call it 'money'.

– David Mamet[2]

"What is truth?"

– Pontius Pilate (John 18:38)[3]

I have a lot of friends who are programmers. The programmers have always gone like, "Those [Bitcoin] guys are crazy." […] And then, almost 100 percent of the time, they sit down, read the paper, read the code – it takes them a couple weeks – and they come out the other side. And they're like: "Oh my god, this is it. This is the big breakthrough. This is the thing we've been waiting for. He solved all the problems. Whoever he is should get the Nobel prize – he's a genius. This is the thing! This is the distributed trust network that the Internet always needed and never had."

– Marc Andreessen[4]

It would be very surprising if [the Bitcoin solution to the Byzantine Generals' Problem] didn't have substantial application. … That something very significant has happened – I think the prospects for that are quite good.

– Larry Summers[5]

Bitcoin is hard to grasp because it's almost like a technology from an alien civilization.

– Ian Bogost[6]

---

[1] Deleuze, Gilles, and Guattari, Félix, Capitalism and Schizophrenia Volume I: Anti-Oedipus.
[2] Heist (2001), David Mamet.
[3] John 18:38
[4] Marc Andreessen interviewed by The Washington Post: http://www.washingtonpost.com/blogs/the-switch/wp/2014/05/21/marc-andreessen-in-20-years-well-talk-about-bitcoin-like-we-talk-about-the-internet-today/
[5] https://www.youtube.com/watch?v=UVGq0zaZsNg&feature=youtu.be
[6] https://www.theatlantic.com/technology/archive/2017/05/blockchain-of-command/528543/

In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions.

– Satoshi Nakamoto[7]

Nullius in verba

– Motto of the Royal Society[8]

[7] 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2008) https://bitcoin.org/bitcoin.pdf

[8] Nullius in verba is commonly translated as "On nobody's word" or "Take nobody's word for it". It formulates the principle of trustlessness at the origin of modern science. The motto dates back to the founding on the Royal Society, in November 1660. It is extracted from Horace's Epistle to Maecenas (his benefactor), in which he apologizes for abandoning lyric poetry for philosophy.

Foreword

§0.00 — Crypto-current exists if secrecy has a trend. Such a suggestion is naturally obscure. It coaxes attention toward the surreptitious direction of things. 'Crypto' is simultaneously the topic, and the retraction of the topic. This evasiveness is compounded by the complexity of its complement. The current eludes docile conformity with the order of objects. This is – apparently – quite independent of any strategic commitment to concealment. It is a flow of time, electricity,[9] and cash – a turbulent conceptual confluence. Current events are the only kind. If we are unable to step into the same current twice, it is because of what irreversibility has secured in the past. A double blockage then – produced, in a stream, as concealment and as sedimentation. Subsequently, everything we have to say here is already over (but unseen).

§0.01 — Is it really necessary to be so cryptic? This question will do, as a trigger. It seems – however querulously – to ask everything our title seeks to, and more than a book is able to comprehensively engage. The implicit reciprocal: Is it not possible to be clear? What begins with a minor irruption of cognitive irritation, agitated by a few specific words, opens into a history of secrecy invested with hazily-discernible momentum, and beyond, into the dark Herakleitean gnosis – matrix and crypt of Occidental philosophy – Φύσις κρύπτεσθαι φιλεῖ ("Nature loves to hide").[10] The provocation of integral obscurity leads to the 10,000 things.

---

[9] Crypto-Current is not, by intention, a book about electricity, but it is quite probably a book about electricity nevertheless. Crypto-current (the thing) works itself out that way, in stubborn obscurity. Electronic publishing is no more than a late phase of its eventuality – although, essentially, among the most conspicuous. Electric current – measured in Ampères or 'amps' – conventionally takes the algebraic symbol 'I', derived from the French intensité de courant (current intensity), as used by Ampère in the formulation of his force law (1820). It is exactly current intensity, apprehended at a superior level of abstraction – and therefore without the benefit of any yet-stabilized, compact notation – that provides our topic. When posed in the Kantian fashion, our question – determined now at a scale that is bound to escape us – asks: How can there be anything like current, in general? It is, of course, time that is put into question here, but in such a way that electricity – and more specifically hyper-electrification – conducts the interrogation. Even within this widened domain, Ohm's Law (1827), $I = V / R$ – current is equal to potential difference over resistance – provides a definition we will not, and actually cannot, find reason to depart from, unless in an abstract direction. Our task, rather, is to generalize it, without subsidence into metaphor. Current is not a figure for something else. It is the thing itself – or real time – even, or perhaps especially, when it is most artificial.

[10] The surviving Fragment 123 of Heraclitus (Φύσις κρύπτεσθαι φιλεῖ) hides much within its natural English translation, Nature loves to hide. A glance at the Greek is required because it is especially important for us to note that concealment is already crypto. In its invocation of a crypsis intrinsic to nature – an integral obscurity – the fragment captures a topic anterior to any dissociation of epistemology from ontology. It evokes an active or strategically self-directed dynamism of the unknown. Concealment is determined as a potency on the side of the

§0.011 — Glimpsed at its distant pole of unbounded abstraction, the cryptic is the ultimate philosophical enticement. At this point of origination, two-and-a-half millennia behind us, philosophy was nothing other than abstract cryptography. Its concern was hiding. If cryptography is currently subsuming philosophy back into itself, the historical figure thus sketched is a great cycle – an obscure return. Restoration – closing an epoch (of financial discretion, most superficially) – is also an irreversible liquidation, into currency. Registered within the terms of the transcendental or critical philosophy, it is a departure from the pseudo-object of 'the present' in the direction of current time.

§0.0111 — Streams run downwards.[11] Engagement with Bitcoin brings us into communication with hidden inclinations, whose indicators mark productions of directionality – gradients, or temporalizations.[12] Between real succession and such abstract inclines there is no difference. Entropy describes such an 'arrow' most basically, but upon this are built a succession of stream-tapping technologies (hydraulic, thermodynamic, informatic), reinforced by directional mechanisms, beginning with clockwork ratchets, and then proceeding – from the early industrial-era – through check-valves, into electronic forward-bias diodes (rectifiers), and software-implementations of one-way or 'trap-door' functions that support asymmetric crypto-processes, and irrevocable contractual commitments. Current emerges from the machinery of time, which is to say from operational asymmetries. 'Flows' are easily – and often lazily – invoked, without even notional attention to their engineering details. Far too much is already understood about the mechanics of irreversibility to leave such vague suggestions as a stopping point.

§0.02 — Economies are assembled from flows. Unsurprisingly, therefore, their native codes are currencies, or current-signs. As societies mobilize matter-energy resource streams, their monetary conventions register these flows by inversion, and strict reciprocity. Hole-flow in electronics is a close analog. Every non-barter commodity exchange, or non-financial transaction, catalyzes a flow, by

---

'object', or rather – far more precisely – the side of 'that' which eludes determination as objectivity, rather than merely a deficiency attributable to the subject. 'How do we know?' is far too confident a question. 'How does it escape knowledge?' interrupts the epistemological presumption. 'Ignorance' is thus construed positively, as a natural production.

[11] In Chinese language and conception, drawn from the practicalities of water clocks, 下 (xià) or down is the direction of the future, while 上 (shàng) or up is that of the past. Temporalization is descent. Water models time, to some degree of adequacy, while also hiding it. As already for the Greeks, and still for us, it in some way flows. If translated into the terms of occidental theology, The Fall never ended. Onwards is down, at least in abstract inclination.

[12] Morgen E. Peck writes: "… a bitcoin miner can … be confident that the other miners are not changing entries on the blockchain, because in Bitcoin there is no going backward." A re-installation of irreversibility is the primary achievement.
http://spectrum.ieee.org/computing/networks/the-future-of-the-web-looks-a-lot-like-bitcoin

pricing it. The 'real economy' is thus automatically captured, by a monetary code, even when – as is overwhelmingly typical – this quantification through signs is never aggregated. Since money systems install an intrinsic economic intelligence (preceding all reflective theorization), economics – uniquely among the sciences – inherits a field of objectivity whose arithmetization has already taken place. This same delicate shadow, cast into business ledgers (pre-denominated by currencies), at once facilitates and registers a system of flows, in a twin production of economic objects. Business is recorded in the way it is produced. Dynamization of the commodity – or economic circulation – is not reducible to, but nevertheless strictly corresponds to, transference of signs.

§0.021 — The economic event, then, is co-original with its semiotic double. It is enabled by signs, before being represented by them. Even the secondary processing, through aggregation, of such information has a pre-theoretical foundation. Powerful economic agencies – most significantly the state's tax authorities – concentrate commercial data, long before scientific political economy begins to re-compile it, as an analytical object. Logos arrives late.

§0.03 — It approaches a truism – although not one for this reason to be glibly dismissed – that philosophy assumes, as if by right, a position of sovereign authority relative to everything it touches upon.[13] A discussion of Bitcoin and Philosophy amounting only to a confirmation of this stance would

[13] Among the nagging contexts of this book is the emergence over recent years of a neo-humanist philosophical school, constituting the dominant development of speculative realism. While specifically differentiated from earlier modes of humanist thinking by its consistent collectivism, it remains deeply conservative in its metaphysical commitment to the irreducibility of reflective human cognition to non-linear machine-process. In this regard, it affirms a species of philosophical writing understood as transcending the algorithm in general, as if – even after Gödel – we could presume to set such limits with confidence. It is a school that resonates with a specific neo-Kantian lineage, inflected terminologically through the work of Wilfrid Sellars, and the resuscitation of a 'space of reasons' irreducible to anything cognizable within the space of a supposedly strictly-bounded 'understanding' that is now carried techno-historically by comparatively informal engineering initiatives and disciplines. That which can be justified, it is asserted, cannot be dissolved into mechanical production, in principle. This claim is both bold, and traditional. By its very nature, it defies all prospect of determinable testing. Since any possible digital sequence is potentially the output of a program (and actually of an infinite number of programs), there cannot be any definite criterion of cognitive competence, when this is formulated in terms of a transcendent rationality. Testable performance is inescapably vulnerable to the prospect of mechanical emulation. Definite criteriology has, therefore, to be surreptitiously side-lined if the algorithm, in general, is to be subjected to philosophical delimitation. Whatever it might possibly be that no 'algorithm' could do, in principle, cannot – in principle – be clear. Critique is demarcation. It sets the limits of a topic (of pure reason, practical reason, and judgment, inaugurally). Crucially, these critical exercises are immanent, i.e. limited to realizable tribunals, or fields of judgment. They mark horizons. No Archimedean position is available to them. They do not ever in reality successfully project beyond themselves, to set the limits of something outside, in an attempt to ensure security against it. In other words, according to a proposal drawn directly from the philosophical tradition, critique has no rigorously conceivable speculative employment. Yet it is exactly some such speculative inflation that is

merit contempt, even if it were packaged as humor. Since any attempt to philosophize about Bitcoin would already be a joke, it is better to get it. Bitcoin seizes philosophical attention because it is already doing philosophy – or what philosophy is still (on ever rarer occasions) expected to do – and at multiple levels. It tells the truth. Bitcoin is not only a recognizable philosophical statement, but also, and more importantly, a philosophical automatism, a synthetic philosophical machine.[14] It not only philosophizes in the manner of a man – although this is its certain prospect – but also finally in the way of an angel, or a lesser god. The 'intellectual intuition' (Intellektuelle Anschauung) that is for Kant a mortal impossibility, is for Bitcoin an operational principle. It is destined to close upon itself, and thus know itself. By becoming time, Bitcoin promises an exhibition of unleashed thought, in a way no introspective anthropology ever can.[15]

§0.031 — Throughout this book, 'philosophy' is employed freely as an abbreviation for 'modern philosophy', which is in turn consistently conceived – tacitly when not overtly – as critique in its (roughly) Kantian sense. To philosophize on any subject over recent centuries, as still today, has been to criticize, in the positive acceptation of this term, by differentiating the transcendental format from the empirical datum, and then resolving – or, stated more realistically, negotiating – the boundary

---

required in order to assert the irreducibility of thinking to complex machine behavior. If this is the only way for philosophy to reproduce its effective cultural dignity, it can be confidently predicted that it will not long survive the techonomic intelligence explosion in which it is factually embedded. Transcendence over against the machine (in general) is the epitome of metaphysical presupposition. Neohumanism, then, is a consistent implicit theme here, as it will be far beyond the bounds of this discussion. It is engaged here, primarily, via a route-around – or an unbound evasion. The bypass operation is the critical current. What cannot be stopped also should not be.

[14] The techonomic horizon, for 'us', coincides with the impending crisis of historically-actualized artificial intelligence. Encapsulated within this by now manifest potential is the comprehensive automation of philosophy. It cannot be simply assumed, therefore, that professional philosophers will respond to the prospect with detached equanimity. The simulation – and thus replacement – of their defining activity is integral to the hypothetical outcome under consideration. Under such circumstances, a coherent defensive reaction is the natural expectation. This is, of course, what we see. We will see much more of it. Yet there can be no stable hierarchy, preserving the superiority of philosophy over against a Critical Automation Theory (of the type advanced, for instance, by Luciana Parisi), or some less explicitly formalized analog. Automation is no more tractable to philosophical reflection, in principle, than philosophy is practically tractable to automation. The dominating considerations in both cases are synthetic, or experimental. A circuitous skepticism balances the technicization of understanding against the understanding of technicity, with both locked into a productive cycle. Learning fuses cybernetically with the machine. There is no Gordian Knot here for traditional authority to sever. Instead, there is a 'question' that cannot be confidently distinguished from an informal technical research program, and which therefore shrugs off non-ambivalent philosophical determination. An armchair philosophical objection carries no serious weight compared to something coming together in the garage.

[15] These will almost certainly seem to be inflated claims, even when attributed to sheer efficient multiplicity. That is why our credence is being effectively bypassed. Modernity has disconnected our doubts from any system of permissions. What cannot be believed is no longer preventable.

conflicts between the two.[16] However it is specifically articulated, critique isolates a properly transcendental productive principle, or function, which is constitutive of a domain rather than existing as an item within one. It thereby marks a unilateral or ontological difference (which is to say, a discrepancy irreducible to any relation between terms that are internal to the domain considered). Critique is, necessarily, the theoretical assertion of a non-empirical partition. Through critical abstraction, the consistent order of the system considered is liberated from its specific instantiation, to become a philosophical preoccupation, immunized against the distractions of any merely factual controversy about its content, but also – simultaneously (or diagonally) – from purely formal considerations of its internal logical organization. It is committed to a zone of positive discovery (which logic cannot be) that is systematically enveloping (as no empirical concern can be). Philosophy, as such, no longer has anything else whatsoever to attend to. If philosophy cannot be critique, it cannot be anything (that matters within Modernity). That is its essential immanent Law.

§0.032 — The target of critique is 'metaphysics' – conceived as a specifiable cognitive error. As determined by Kant, at the origin of the transcendental-critical enterprise, metaphysics is understood as the systematic attempt to apprehend ('transcendental' or ultimate) conditions of objectivity as if they were themselves objects. The repudiation of this effort can be summarized with approximate adequacy in a phrase that serves as a critical war cry: objectivity is not itself an object. This is to borrow freely from the critical framing of metaphysical error as it is found, compactly formulated, in the Heideggerian

[16] Transcendental-empirical difference is very far from being an uncontroversial conceptual commitment. Within the Anglophone world, its most celebrated critic has been Willard Van Orman Quine, whose 'Two Dogmas of Empiricism' (1951) assaults the conceptual foundations of analyticity. Logical identity cannot find secure grounds in definition, Quine argues. The lexicographic features of any term are never simply given, but must always be produced. Language has no meta-level logical characteristics, capable of securing analytical judgments. Along these lines, an attempted re-absorption of the critical impulse into an expended empiricism has been the dominant Anglophone response to the transcendental blueprint for the modernization of philosophy. Such an approach coordinates well with the techno-empiricism of the computer age, in which programs are processed as data. Between codes and information, protocols and applications, there can be no logically secure hierarchy, once Turing-complete digital computation is at work. Yet, from the partial perspective of the crypto-current, it is obligatory nevertheless to dissent. The resilient value of the analytic-synthetic distinction lies in its emphatic asymmetry. That is 'analytic' which can be conveniently checked, while the 'synthetic' has to be laboriously discovered. Cryptography essentially coincides with this distinction. We are thus, in passing, compelled to dismiss Kant's identification of synthesis with simple addition ("7 + 5 = 12") as misconceived, and misleading. It makes no sense to discuss the analytic, or synthetic, except in regard to reciprocal asymmetric operations, exemplified by trap-door functions. In the most significant instance, the analytic-synthetic divide runs between arithmetical production and factorization. The rigorous content of the distinction is work, in the sense given to this term by computer science. Its entire domain is exhausted by twin procedures of asymmetric facility. In its scientific application, it divides theoretical construction from experimental replication (or, once again, discovery from checking). Nature only has definite secrets in respect to this split method. If 'thinking' – or experimental discovery – were as economical as testing, or attempted result replication, there could be nothing like science at all.

'fundamental ontological' re-statement of transcendental philosophy. Being is not a being.[17] More significantly, for our current purposes, it can be conveniently extended to apply to contemporary techno-social arrangements and communications apparatuses by way of a comparatively simple translation protocol. 'Metaphysics' – over against which disciplined philosophical critique emerges antagonistically – is instantiated by any identification of a systemic function with some node internal to the system considered. It can therefore be readily seen that the 'flattening' of a network, through the elimination of system-critical, concentrated, indispensable nodes, which is to say through the distribution of its efficient principle, is an exact – if abstract – execution of a critical operation in the Kantian sense. A network is a critique.[18]

§0.04 — Already, at the most naïve level of its acceptation, 'Bitcoin' is a word that refers to at least three things. Of these, the most elementary – although today least invoked as a definition of the term – is a succinct, technical paper, in whose catalytic code everything was, in a certain sense, already implicit. There is nothing obvious about this terminological development. To speak of the 'critique of pure reason' is first of all to name a book, even though (no less than with Bitcoin) it is the book's 'object' that is being named. Critique of pure reason (the 'thing') is in this case a delayed signification, despite the fact the title says nothing else. In the case of Bitcoin, this system of acceptations is conspicuously inverted. 'Bitcoin' is not understood primarily as a paper,[19] perhaps because it is not

[17] For the purposes of its employment here, 'ontological difference' (between Being and beings) is considered to be no more than a restatement of transcendental-empirical difference, of negligible philosophical originality. It is not adopted as a marker of penetrating inquiry, therefore – still less of Heidegger scholarship – but solely as a resource valued for its pedagogical practicality. The term is validated for this purpose precisely insofar as the structural integrity of critique is economically conserved by it. Being is not a being. In this formula, the basic transcendental insight is captured with what is probably unsurpassable economy.

[18] Critique is anti-Archimedean philosophy, and in this strict sense an intrinsic anti-rationalism. It is directed against the pretensions to super-ordinate theoretical leverage which define metaphysics. Every claim to exception from immanence falls prey to it. Its sole empirically exorbitant proposition is that the whole permits no oversight. No 'view from above' can be true. Critique thus supplies the schema for that flat epistemology which empiricism requires and fails, itself, to produce. Its historical mission is to make the world safe for empiricism (i.e. techno-science). It can therefore be understood as modernity's watchdog. Liberal civilization knows no higher principle of security. Its enemies are 'churches' with global ambitions, which is to say universalizing abstract-ecclesiastical authorities. When all relevant terms are stripped of encrustation with maximum rigor, critique is accurately characterized as anarchism in philosophy. It is that, alone, which cannot know any higher law. Whatever tries to transcend it can only repeat it, or less. We call this time, which can never be anticipated or out-lasted. Above Temporalization there is nothing. To engage in critique is to think in the name of time.

[19] The word 'paper' slides easily into the digression queue. After all, it might be convincingly argued that reference to the 'Bitcoin paper' has already surrendered to a linguistic legacy of peculiar inappropriateness, and thus to laughable anachronism. 'Paperlessness' is a retrofutural and thus historically ironized idealization of the electronic landscape. It is either pseudo-teleology or – far more probably – premature forecast, tacitly engaged by this and any other discussion of digital information, even prior to a collision with the thematic juggernaut of 'paper'

primarily an argument. Its nexus of persuasion has migrated outward, in close association with the meaning of code. Critique undergoes accelerating automation.

§0.041 — The philosophically pressing motive for hesitation – however momentary – at this point of origin, where the balance between the virtual and the actual is most dramatically precarious, is to hold open the question of primordial introduction, even as it tends to eclipse itself. Already, during this remarkably brief embryonic phase, when Bitcoin was implemented only in words, it was at least double – at once a title and a topic. From the beginning, the term pointed beyond the name of a text, towards a virtual entity, something that could be made to happen, or that was, in being rigorously outlined, already being made to happen. In being drafted, it was in fact initiated – even released – and through its 'preliminary' scripting it had already been informally pre-programmed, or practically introduced. Bitcoin has existed from the moment it was named (and its origin could be pushed still further back). Such occult potentiation of the semiotic event is what it is to code, in the modern sense of this term. It is something much more than description. As code, writing is transported beyond representation to an operational horizon, where it builds what it says, immediately. Language that cannot follow it along this path is already a husk – inconsequential by essence – unless politics can save it. (Bitcoin is the bet that it cannot.)

§0.042 — Even when not explicitly referencing a text, and thus evoking the gap between word and thing, the name 'Bitcoin' remains divided by a fatal difference (one of still greater importance to our discussion). The initial, narrow, version of this rift – distinguishing any quantity of bitcoins from the comprehensive singularity of Bitcoin – is a critical faultline to which we will repeatedly return.[20] It anticipates – while remaining irreducible to – a schism, of gathering social concreteness and historical consequence, opened by the polarization of 'Bitcoin' (conceived as specific, contingent, branded, and politically- or competitively-extinguishable) over against 'the blockchain' (a generic technological innovation, that is accepted as irreversible, and promoted as conservatively-assimilable). Threading through the most energized Bitcoin debates is a question of limitation. Can the currency system be

---

money. If 'papers' are still with us – even when they have only ever been incidentally propagated in a 'dead tree' medium – it is because history is a loose sheaf, rather than a neat stack. Since technological epochs co-exist, simultaneously, anachronism finds its avenues in space, even more than in time.

[20] The distinction between "lowercase bitcoin and Initial-Cap Bitcoin" (in the words of Terrence Yang), i.e. "digital money" and "a protocol" respectively, has already been impressively standardized. The emulation of a philosophical difference – and, as moderns, we can confidently say the philosophical difference – by a terminological convention rapidly settled within the worlds of technological commentary and financial news media attests to a determination of conceptuality from the outside. The 'thought' that matters is produced in advance of any explicitly philosophical apprehension. (This fatality will no doubt evoke Hegel's "Owl of Minerva" among those receptive to speculative communization, whose problems will be touched upon later in this book.) For Terrence Yang's articulation of Bitcoin's ontological difference, see.

circumscribed (and then transcended), as the larval stage of something greater than itself – serving as the historical 'bootloader' for a new Internet revolution driven by generic blockchain-based trustless transactions protocols? The philosophical rift re-activating transcendental-empirical difference in the domain of monetary technology has thus already been dramatically opened and even tentatively evaluated in the course of a process of widely-reported, financially-invested, socio-economic exploration, before any self-conscious philosophical activity reaches it. During the elaboration of this controversy, some of the crucial interests at stake in Bitcoin's inner rift have been exposed, and their theoretical absorption facilitated. The fact that the question has been raised by opportunistic venture capital does nothing at all to detract from its perfectly philosophical character, as captured – with reasonable fidelity – by the formulation: What are the limits of Bitcoin?

§0.043 — It is at the third – and fully historical – level of meaning, however, that the ultimate scope of Bitcoin's significance is gradually manifested. Beyond the initial formulation (or abstract protocol), and its subsequent implementation as a functioning currency system (and already something more), there emerges a far broader Bitcoin installation process,[21] of evidently vast but still-obscure character and magnitude. The formula is a diagram, the implementation is an active database supporting a crypto-currency, but what undergoes installation is an entire techonomic 'ecology' or 'infrastructure' – a

[21] Eminent wave theorist Carlota Perez insists upon the historical integrity of technology and finance within 'great surges of development', each of which introduces a new 'techno-economic paradigm'. She first divides each surge into an 'installation phase' and a 'deployment phase' (each in turn is tractable to binary sub-division), noting that the transition from one to the other is typically marked by an investment-overshoot driven financial crisis. Political economy is a rhythm. Its pulse, with roughly half-century periodicity, encompasses not only techno-industrial innovation and its financing, but also social sentiment and political animation. The history of capitalism is thus constructed as a succession of comparatively discrete stages. Each of Perez's 'great surges of development' corresponds to a complex telic object. The language of 'installation' already says as much. Some virtual thing arrives, or is put into place. (These terminologies are strictly inter-changeable.) On the basis of the most mechanical reading of Perez's supple analytical framework, something corresponding to a Bitcoin 'deployment phase' might be expected in the 2030-2040s. Such a time-table assumes an absence of techonomic acceleration at the deepest level of the modernization: a negative prediction which Perez's historical analysis as a whole supports. The Great Waves of development are paced by an anthropomorphic-generational temporality, rather than a self-propelling momentum inherent to mechanical industrialism. They are not speeding up. Comparatively stable periodicity is essential to the hypothesis. Crypto-Current is not a documentation of the Bitcoin installation process, although it grants – without reservation – the potential value of such a work. There is perhaps nothing that would more incisively capture the deepest principles of the rising capitalist wave. Functional trustlessness, as an industrial output, remains only very tentatively conceived. The momentum behind it is difficult to easily overestimate. With the emergence of Bitcoin, rigorously constitutional governance, a political-economic problem that the old liberal order found impossible to successfully navigate, has transitioned into a techonomic capability under automatic propulsion. Industrialization of government is the definite implication. Quite clearly, the socio-political stake in a capitalist development wave can never have been higher. Regimes, potentially, are now business outputs.

complex manifold of interlocking parts, whose horizons are still lost to us in hazy distances (however rapidly we are hurtling into them). It is on this dimension that Bitcoin and Philosophy is most clearly and comprehensively overwhelmed. After being thought, and then done, Bitcoin promises – or threatens – to change the way everything is thought and done, or would be thought to do so, were it not that in the age of code such dulled terms have outlived their usefulness, and persist only through inertia.

§0.05 — Bitcoin machines value. It follows that the prevailing conception of technology as instrumental capability, subsumed under extrinsic ends, is among the very many things to fall by the wayside as the process escalates. Traditional categories of thought (or conception) and action (or performance) are mutually subsumed into an irreducible cognitive action. The strengthening diagonal current passing between the notional and the actual, 'ought' and 'is', intelligence and mechanism – which in its aporetic articulation has been the exquisite torture of postmodern philosophy – is simply code. Bitcoin ushers this cryptic fatality into simultaneous conceptual and mechanical consummation.

§0.051 — It is necessary to go further. In the final analysis, nothing less than the nature of reality is brought into question by this event. It concerns the 'Being of beings' (at least). If the claim seems extravagant, it is nevertheless inescapable, once the transcendental status of an ultimate criterion based upon absolute succession is granted to the Bitcoin protocol. It is not only that no higher tribunal exists. When envisaged at a sufficient level of abstraction, no higher tribunal could possibly exist. The Bitcoin ledger is the first intrinsically reliable record. It is now known what happened, without argument. This is a situation without precedent which also reaches – immediately – an absolute limit, in principle. It thus exemplifies the synthetic a priori. There is no philosophical thinking of Bitcoin – in either the subjective or objective genitive – that is not also ('simultaneously') a re-thinking of time, or sovereign decision. 'Re-thinking' is a revision, but no less a restoration. Bitcoin introduces us to a time-machine, or time-synthesizer, which can only complicate any initial intuitions about its novelty. It has been on the way for centuries (at least). This will, in any case, constitute the stubborn, guiding assertion of the book.

§0.06 — Crypto-Current is organized into six sections, which together compose a cycle. The analytically dismantled circuit of Bitcoin – with each segment seized as a philosophical provocation – finally closes upon itself in an attestation of its positive groundlessness. The loop of Bitcoin auto-production knows nothing of transcendence, at any stage. Whatever might have sought to intrude, representing an extrinsic authority, is dismissed as a superfluous 'trusted third party'. The circuit is the entire thing.

§0.061 — On the path to a philosophical hash of Bitcoin as a transcendental horizon, Crypto-Current commits itself to a number of interlocking but isolable propositions. Among these, the most intensely

exploited – which is to say, those found indispensable for our purposes – are advanced here, in the approximate order of their introduction. Compressed in this way, they can only appear ill-grounded, or dogmatic. They are anticipated in this way for the purposes of convenient preparation, not persuasion. (Digits in the first decimal place correspond to the chapters of this book where the principal discussion is found.)

§0.1 — Chapter One provides an introduction. It takes a short Satoshi Nakamoto text[22] as its point of departure, in order to capture Bitcoin as larva.[23] Its intimate relation with the history of cryptography is supplemented by something hidden, working out through it. Word becomes code.

§0.11 — At the beginning there is a yet-underestimated philosophical work. Whatever happens to Bitcoin, its status as a decisively important document will be secure. Furthermore, reflexively, what is meant by a 'document' will never again be the same, after logical envelopment by the category of the ledger entry. Documentation has crossed a new threshold of mechanization. Bitcoin the documentary is thus an exposé in which nothing is hidden, unless behind a fully-manifested mask. It binds publicity to security. All Bitcoin does is secure documentation, which is enough.

§0.12 — The entire cycle is captured by this preliminary diagram, as an "electronic cash system". In the closure of this cycle, a rupture – or irreversible occurrence – has taken place, comparable in structure and scale to Gödelian transcendental arithmetic, and to Public Key Encryption. Money changes phase, with an abrupt radicality from which there can be no return.

§0.2 — Chapter Two explores the reciprocal application of transcendental philosophy and the Bitcoin protocol to each other. It is proposed that the critical triple skein of ontological difference, subtraction of transcendence, and temporalization can be pursued, without significant interruption, into the analysis of Bitcoin. It takes Satoshi Nakamoto's (2008) Bitcoin paper as its basic text, since this is what the word Bitcoin – by informally-standardized cultural convention – names.

§0.21 — Bitcoin is first broached as a philosophical topic, and thus, subsequently, as a mode of philosophical access to other things. Philosophy is required to concede much, in following this track, especially in regard to the traditionally-conceived cultural and institutional bases of its own authority. The order of discussion follows the course of the problem – the double-spending problem (DSP) as it is nominated – which is understood critically, not only as a practical obstacle to functional cryptographic currency, but also as a philosophical topic of radical generality. Duplicity in its deepest

[22] Bitcoin P2P e-cash paper' (2008/11/01)
https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html
[23] A larva is a mask, and a cryptic (infolded) potentiality.

and broadest sense is the target.[24] The DSP cannot be resolved, then, without simultaneously bringing singularity into the fold of formal engineering. The concrete execution of the Bitcoin protocol provides a peculiarly vivid demonstration of the socio-technical (machinic, or techonomic) production of abstract singularities. Anything else would be cheating.

§0.211 — Critique – the critique of metaphysics – is philosophy (as a current undertaking). It is what philosophy has irreversibly become. Insofar as these terms still diverge, however minutely, there is a task that remains uncompleted. Philosophy establishes itself in modernity by way of auto-critique. 'Like' Capital it is a path with firm direction, but without destination (the path is the destination). It exists only by perpetually overcoming itself. Critical – or diagonal – method is a tool through which philosophy is definitively exhausted. Its sole product is immanence. The rigorously complementary formulation asserts: Residual transcendence is the negative of the philosophical undertaking. The systematization of the synthetic a priori is the model of diagonalization in philosophy. Bitcoin is therefore in the very strictest sense a critical enterprise, targeting "trusted third parties" as superfluous metaphysical structures. Immanence is its techonomic – or socio-historical – rather than its merely reflective-conceptual output (or production).

§0.2111 — Critical method coincides exactly with diagonal argument. It identifies pseudo-tautologies and proceeds through their complementary pseudo-paradoxes. The synthetic a priori is the model. Circuits are diagonals.[25] They do not resolve in one way or another, but always between, either in a hunt for equilibrium, or a flight through inter-excitation.

§0.22 — Analytic-synthetic difference registers cryptographic asymmetry within philosophy. It marks the irreversible. In keeping with the mainstream critical tradition, the formulation of methodical procedure is subsumed into the problem of time. The philosophical problem of time, it might be said, if this were not an invitation to misunderstanding. Restoration of transcendental temporality, or absolute succession, is a philosophical achievement only insofar as the process of philosophy has been thoroughly dis-anthropomorphized, technicized, economized, and (thus) spontaneously materialized. The realization of the idea is only accomplished in the machine. Auto-materialization is so essential to the critical process that it amounts to an intrinsic destiny. Critique cannot consolidate itself other than

---

[24] Duplicity is not merely error, but the malicious instigation of error. Once again, cryptography schools philosophy in realism here. 'Confusion' is, in this case, primarily enemy action. An effective response therefore exceeds epistemology, or cognitive self-correction. Doubling spending is more than a mistake. The requirement is not only for intellectual adjustment, but for a procedure that automatically secures resilient singularity, against attack. Knowledge is situated on a battlefield. It is this that constitutes Bitcoin's principal achievement.

[25] "I think this is a reference to Bishop in Aliens," suggested the anonymous 'ClarkHat' ingeniously, when this proposition was initially floated on Twitter. (Such entirely supplementary semiotic production exemplifies the surplus value of code.)

as historical modernity. It would be a redundancy, or merely emphatic, to add: in reality. Mechanization is nothing but mechanization in reality, and in fact compresses further, to sheer realization, or production.

§0.221 — Natural philosophy – which achieves intellectual autonomy as physics – lies directly in the path of the question of time. In particular, it has radically re-framed transcendental aesthetic within cosmological spacetime, where absolute temporality finds no place. Bitcoin can only interrupt this apparent tendency to theoretical detemporalization, since there can be no resolution of the DSP without strictly determinable succession. Bitcoin and time restoration are finally indistinguishable.

§0.23 — Network thinking – as instantiated by the Bitcoin protocol – complies with the pre-eminent contemporary operationalization of transcendental philosophy (which is considered here, with a maximum of strategic vehemence, to be exactly synonymous with critique). A reliable expectation follows, that Internet production is accompanied by format / data differentiation (into 'layers'), eradication of transcendence (absence of 'critical' nodes), and temporalization (primordial production of absolute succession, or post-relativistic order). The network – radically conceived – is a quasi-teleological manifestation, tending towards the actualization of a principle that is itself emergent, and which functions as a criterion of intelligibility.[26] In consequence, any network can be evaluated with reference to an abstract model of self-reproducing decentralization. Bitcoin exemplifies – which is to say realizes – this process with exceptional starkness.

§0.3 — Chapter Three engages semiotics – or signs about signs. It concentrates upon the status of Bitcoin as a solution to the double spending problem (or 'DSP'). A case is made for the extreme generality of the DSP as a practical semiotic quandary, roughly coextensive with the existence of life. Resolution of the DSP through a crypto-secure proof-of-work protocol is thus an episode in terrestrial bio-history, and not merely a drastic anthropological – or mature industrial capitalist – innovation (even if it is also both of these). What the protocol addresses is no less than virus, in its broadest extension. It corrects the intrinsic economic crisis of the sign. Semiotic values are instructions, and necessarily

[26] Given sufficient – i.e. radical – critical correction of classical conceptions, the network is an Idea in the strong (Platonic) sense and, still more definitely, an Aristotelian causally-efficient End (telos). It allows for judgments of adequate approximation and actualization, respectively. Subtraction of super-ordinate instances – i.e. metaphysical impositions – is the criterion, in either case. Through elimination of privileged or commanding nodes, a network is unambiguously improved, relative to its model. It is no less unambiguously enhanced relative to its intrinsic finality. Flatness is the ideal, and the goal. This is not, of course, to be confused with any psychological conception of purpose, or adequation. It is 'merely' the directive influence of equilibrium, or – to invoke a more recent coinage – 'attractor states' upon the partially-coherent evolution of a system. There are better (or worse) networks, independent of any reference to subjective judgment. In consequence, there is a real gradient to modern history. Only at the most superficial level of evaluation is Bitcoin a popularity contest. The conflict it survives is far more serious.

coinages. They make a difference, of 'economic' consequence. Duplicity – 'hijacking' – is thus automatically incentivized. To capture instructions is to command resources. This strategic option is no younger than the organism.[27]

§0.31 — Potential duplicity is a foundational semiotic concept, with extension far beyond the anthropomophic sphere. Virus already effectuates it (without any recourse to metaphor). The sensitivity of any system to code is, primordially, a vulnerability to capture. The programmable is the reprogrammable. Zoosemiotics is enveloped by this dilemma. No organism that takes advantage of clues, or cues, escapes their strategic ambiguity. Reading risks misreading essentially, and long before language. The hazard of trickery, by mimics, or deceivers, was not an invention of man, still less of digital information systems.

§0.32 — Spam, nevertheless, dramatizes the inherent tendency of the duplicitous sign with peculiar sharpness. It is no coincidence that the genesis of Bitcoin is deeply-interconnected with the practical problem of spam filtration. Spam experimentally demonstrates anti-money. In this, it has been a great teacher. Any functional system of message value credentials, negatively determined against spam, is already an embryonic digital currency.

§0.33 — Robust credential production makes money, whose ultimate basis is counter-duplicity. Bitcoin variants, or 'alt-coins', belong firmly to the same field of problems. Alt-coins are, at least partially, duplications – quasi-copies, or rough clones. The superiority of Bitcoin, in respect to competitive 'alt-coins' can rest only in its originality, or 'first-mover' advantage, since nothing precludes the emergence of a perfect copy. The eventuation of network effects – i.e. raw or irreducible singularity – does everything. Coinage has no essence beyond its event. From an exact date, something happens. There is no doubt more that can be said, but it cannot stretch to full-specification of the phenomenon, even in principle. Bitcoin is, both rigorously and redundantly (or in multiple senses), a production of singularity. Non-duplicity captures this in its most generically-intelligible dimension. A DSP-solution defines a semiotic, irreducible to the signifier or the index (to sense or reference), and already tacit in the nature of the monetary sign.

§0.34 — Explication of the 'double spending problem' (or 'DSP') necessarily produces, or reproduces, an economic theory of the sign. It restores exclusivity, or – in the language of the economists – the rivalrous sense of the semiotic entity, as commercial token. Resolution of double spending can only be a compression to singularity, as grammatical function and implicit concept, but more basically as

[27] Deleuze & Guattari thematize this topic as the surplus value of code, as illustrated by the sexual instruction capture, or hacking, of the wasp by the orchid. The sign, duplicity, and resource acquisition are compactly integrated within the very widespread phenomenon of mimicry.

practical resource. The conservation of value establishes its real and intrinsic – i.e. autonomous – ground. In this way (alone) it establishes its conditions of existence, in a circuit, by resourcing itself.

§0.35 — The generality of the DSP is evident in many other dimensions. The double opens the door to proliferation without limit. In this respect, double-spending invokes the double of the doubling period, rather than that of double-checking, or double-entry book-keeping, both of which figure on the other side of the account. According to the defining procedure of double-entry book-keeping, whenever money is added, on one side of a ledger, it is subtracted on the other. This requirement implements a distinctive semiotic procedure, irreducible to either signification or designation, which can be named allocation. It is only with regard to its allocative function that a sign can be spent, which is also to say, function as a rivalrous good in the economic sense. To transmit a sign, while still keeping it, in the fashion of language, is the essence of the DSP. A DSP solution, such as Bitcoin, is therefore – by necessity – an assault upon the linguistic model of the sign. Money is not a language. Insofar as it rises to prominence within semiotic theory, it necessarily dethrones the linguistic ideal. Within the anthropomorphic domain, it is precisely in becoming non-linguistic, and non-representational, that signs start to work. Signs are operators, which makes them worth stealing. They are keys, or passes. Virus grasped this more than three billion years ago.

§0.4 — Chapter Four approaches Bitcoin as a contribution to – and problem for – the theory of games. Such a contextualization is ineluctable. The Byzantine Generals' problem, which prompts the Bitcoin solution, is a model game-theoretic quandary, situated within the project of formalizing distributed coordination, which has accompanied Modernity from its inception.

§0.41 — The Bitcoin protocol is designed as a game. Incentives are built into its infrastructure. It only works when it is played. The distinctive feature of the Bitcoin game is that it produces binding decisions without a referee, or dependence upon prior agreement. Coordination is neither presumed, nor invoked, but produced. The absence of all superior authority makes Bitcoin transcendental in the philosophical sense, and adapts it to anarchy in the rigorous sense this term carries in the field of international relations theory. Any player is welcome to cheat. No moves that are possible are forbidden. Do your worst is its open invitation. This is what trustlessness means.

§0.42 — Social analysis is a regional application of game-theory. There is no conception of 'the social' extricable from the domain of games. Transcendental philosophy can be hashed into a game-theoretically tractable vocabulary, which facilitates its general social application. The meaning of 'spontaneous order' is finally indissociable from, and co-elaborating with, that of 'games'. In both cases, what is posed is the strategic problem of multiplicity, or primordial non-coordination. War, politics, and formalized commerce stack successively upon it.

§0.421 — Consensus, as technically formalized within Bitcoin, is game-theoretic coordination, or the solution to a collective action problem. It thus unlocks the most basic problems of social science. Money games, especially, require hard commitments. The DSP is conceived in these (game-theoretic) terms as revisability. It is the negative of a hard, or irrevocable, commitment. Unambiguous irrevocability, then, sets the Bitcoin engineering problem. Lock-in is its specialism.

§0.422 — More particularly, the whole of Bitcoin politics belongs here, including both the conflicts over and within the crypto-currency. From the side of Bitcoin, the initial and framing challenge of the game is to get itself played. This unfolds 'in the rough' where (to mix metaphors) 'turning over the table' remains an option, at least in appearance.

§0.4221 — There is necessarily a question, defining of the left in this domain, whether Bitcoin should be allowed at all. The ideologically basic issue is permission. At this level, the game is existential for Bitcoin, and everything it carries, meaning the occult liberal tradition.[28] Mere survival counts as a win. If permissionless process can establish itself, a great veto is irreversibly nullified. The political sphere is downsized.

§0.4222 — If this trend were not resisted, liberalism would have no enemies. Prevention of Bitcoin, however, looks to be already a lost cause. What Bitcoin essentially is cannot easily be distinguished from this anticipated outcome (which is to say, from its bare survival). Existential security was baked into the protocol originally.

§0.4223 — If rejection proves impractical, might there be moderation? 'Within' Bitcoin itself, there is almost everything to play for. Crypto-destiny appears to bifurcate, even before it forks. The relevant spectrum of variation separates Mainstreamers from Ultras. The dominant topic here is assimilation or, reciprocally, regime change. Is Bitcoin a tool, or a weapon? This question is folded into Bitcoin's Block-Size War, which is as important as any conflict of our age.

§0.5 — Chapter Five is concerned with the function of Bitcoin as money. Theoretical articulation of this problem requires a transcendental deduction of money, as the condition of possibility for commercial calculation. Within this deduction, the six traditional 'qualities' of money – durability, scarcity, divisibility, communicability, fungibility, and verifiability – occupy the place of structurally-inevitable forms, or categories. In other words, and with some qualification, they are predictable (a priori) aspects of money, rather than its mere empirical features. They are mathematically conditioned, and only occasioned by historical causality. Once grasped conceptually, they are confidently expected.

---

[28] That the term "occult liberal tradition" conservatively re-phrases crypto-current is not meant as a secret here. Between liberalization in reality (rather than declaration) and the practical history of cryptography, there is no difference. As the Ancien Régime already knew, Illuminism provides the dramatic mask.

Nothing could be money otherwise (with only notably bizarre exceptions). It follows (in accordance with a priori synthesis) that a robust cryptocurrency will take the form of artificial gold.

§0.51 — Money has six categories. The three indispensable monetary functions – as a store of value, means of exchange, and unit of account – are presumed to be structurally indispensable to this analysis. They are diagonally complicated by stock and flow (the pseudo-synonyms of value storage and exchange), to generate an architectural principle.

§0.511 — The concept of money is not rigorously delimitable. For essential reasons, it has never been captured by a definite idea. We still do not know what money can do.

§0.52 — The story of money – which coincides closely with history as such – can be told in many different ways. There are primarily anthropological, economic, technological, and political versions, among others. Crypto-Current tells a number of these, very briefly.

§0.53 — Abstraction emerges within the historical process, as an immanent product. The monetization of human societies during the Axial Age (~2,500 BC) inaugurates it, triggering the innovation of philosophical and mathematical thought. Money thus conditions the birth of philosophy before becoming a philosophical object, and mathematizes before becoming a regional application for mathematics.[29]

§0.531 — Money thinks. In fact, it out-thinks us, insofar as reflection is brought to it late, after its own cognitive operation has been long at work, and ultimately perhaps also in other ways, yet to be apprehended (from our side). It has already made sense of things, before we have begun to make sense of it. We have no grounds upon which to affirm, with confidence, that money and general intelligence can be finally distinguished. The institutional separation between artificial intelligence research and crypto-currency innovation is not rooted in philosophical principle.[30] The expectation that catallaxy, distributed commercial learning, or price discovery encounters a limit short of the question of the price of being finds its sole resilient foundation in moral indignation. Since Bitcoin demonstrably does ontology, and even 'fundamental ontology', the status of normative revulsion in this domain is irredeemably dubious.

§0.532 — Having yet to think money, beyond a preliminary stage, we are poorly positioned to set hard boundaries around what money itself can think. Meditations upon the ultimate conceptual relation

[29] References to the lineage of this idea (most recently relayed through the work of David Graeber), which is entirely non-original to this volume, are included in the body of the text.

[30] That the commercial process is, from the start, artificial intelligence production is a long-standing suspicion within the Austrian economic tradition. For a recent example, from Hunter Hastings, see: https://mises.org/library/entrepreneurial-super-intelligence-praxeology-age-ai

between money and social identity are inhibited – or interrupted – by an indignant retraction of self from configurations of crystallized value. Yet money, already pre-empts this recoil, and with greater effectiveness, through its insinuation of liquidity, and consequent socio-cultural intensifications of liquidization, liquification, and liquidation. All that is solid melts into a liquid, wherever money touches it. Money dissolves stuff. Currency says this, realistically. To be insulted by monetary denomination of sacralized values, then, is to assume far too much. There is a definite metaphysics at work here, which is to say an image or objectification of money that cannot survive critical scrutiny, or – more importantly – critical social process.

§0.533 — Our dominant models are undergoing rapid obsolescence. For instance, money does not reduce to the concept of credit, even though this reduction has made itself – at least momentarily – inevitable. As the most recent and most complex episode in the history of money, financialization dominates its contemporary conceptualization, and this development was, until very recently, expected to further escalate in the same direction, determined increasingly by invisibility, credit facilitation, and institutional trust. Money appeared to be converging with the function of a bank account.[31] This apparent teleology – guided to invisibility – was extraordinarily vivid. Crypto-currency ironizes and derails it. This is why the history of money has now to be retold.

§0.6 — Chapter Six closes the Bitcoin cycle, by attending to the absorption of socio-economic identity into cryptography, the matrix of philosophy. The Bitcoin wallet is a mask. Asymmetric cryptography formalizes irreversibility at an unprecedented level of techonomic intensity. It initiates the age of the open secret (or of masks). Bitcoin is its currency.

§0.61 — Cryptography envelops philosophy, in reality. The practical processing of secrecy defines a transcendental horizon. Epistemology is broken by its own naivety when it assumes an object without intrinsic impulse to escape. To know is to capture, grasp, or seize. It is thus, at least roughly, to fight.[32]

---

[31] It will entertain future historians that science fiction money was so often denominated in credits. Financialization makes money, fundamentally, a ledger entry, with physical cash tokens marginalized as anomalous relics. To use money is to access an account. As a digital emulation of gold, instantiated upon a public ledger, Bitcoin insolubly fuses primitive and futuristic elements. It exemplifies an alternative financialization, hostile to institutional discretion. There is not retreat from the identification of money with its registration upon a ledger, but rather a radicalization. Yet at the same time its characterization as credit (i.e. bank money) is brought into extreme practical question. The distinction amounts primarily to the subtraction of discretion, which eliminates fractional reserve money creation. The modern bank account is not only a (comparatively complex) ledger entry, but also a permission to borrow, defined by a credit limit. Bitcoin, in contrast, restores money to a positive asset, without counter-party obligation, economically equivalent to abstract precious metal.

[32] Perhaps Francis Bacon never proposed that nature be "hounded in her wanderings and put on the rack and tortured for her secrets." Regardless, the culturally long-sustained plausibility of this quote is itself suggestive.

Bitcoin, whose lineage is cryptographic, inherits better instincts – by far – in respect to knowledge, and truth than those typifying professional philosophy. It expects trouble, and not only difficulty. Its technical specifications are strategic, at the root. Rather than seeking shelter, Bitcoin makes cryptographic attack an intrinsic part of its security infrastructure. Its miners are poachers made game-keepers.

§0.62 — The twin-key cryptography which Bitcoin builds upon is a philosophical innovation of extraordinary – and still enormously under-estimated – importance. Recursively, it is itself a key, to the secrets of the dyad. The crudity of dialectical and structural articulations is comical in comparison. The cryptographic lineage directs application of this machinery, initially, to the public / private distinction, which it practically and conceptually solves.

§0.63 — Bitcoin significantly accommodates agent-identities to the rising Age of Masks, in which digital avatars implement the 'empirical ego' of transcendental philosophy. Identity, address, and account ('wallet') are brought into exact coincidence. All are a single fully-publicized disguise.

§0.64 — The concept of property remained weakly defined prior to the age of advanced cryptography, and the rigorous abstract determination of keys.[33] It is upon lockings and unlockings that the entire reality of property is built. When critically collapsed onto the plane of cryptographic immanence, privacy and property are indistinguishable. Both are accounted in keys. No other valuables in reality exist.

§0.65 — Asymmetry, as operationalized within public key crypto-systems, is an implementation of time – a temporalization, or current. Things go one way rather than another. It is cryptography, then, finally, that unlocks the historical meaning of philosophy, by retrieving the keys of time. Bitcoin realizes absolute succession as accomplished artifice. The cycle is closed.

§0.71 — Three appendices are gathered in the penultimate section of the book. The first is devoted to a slightly larger reading of the Satoshi Nakamoto Bitcoin paper than that undertaken in Chapter-3. The second, folded into two sub-divisions, engages diagonal method (the principal procedure of modern philosophy), and its application to the techonomic integrity of the modern industrial process. The third

---

Secrecy, and not mere ignorance, was the topic. The object of systematic knowledge was recognized as positively elusive. Modernity in science germinated in realistic soil.

[33] The historical precursor to the cryptographic key is the seal. Between the two, the functional analogy is striking, but a seal falls short of a crypto-key due to its dependence upon transcendent authorization. Seals distribute permissions, not capabilities. A seal does not protect itself. It presupposes an extraneous apparatus of authority and enforcement. In this respect, the comparison to the pre-cryptographic history of property rights and protections is only strengthened. What crypto-protection affords, sealing the first true property, is immanent security. The demand for cooperation is relieved.

discusses the geopolitics of Bitcoin in reference to concrete contemporary issues of currency hegemony, the status of the US Dollar, and the economic rise of China.

§0.72 — The apparatus includes a Bitcoin Time-Line, very short briefings on Coins, Organizations, and People, a Glossary, and References. This information is suggestive, more than exhaustive. The scale of the crypto-currency phenomenon already exceeds any realistic prospect of comprehensive purchase, or fine-grained general introduction.

§0.8 — Finally (but also before), there's another thing. It might even be regarded as the main thread. Historically, it will have been. We can be exorbitantly confident about that, with such anticipation being the entire point. There is something more than a progressive causal series at stake in the arrival of Bitcoin. Preliminarily – and from historical necessity – this concern proceeds under the sign of teleology. It has to be noted clearly from the beginning, however, that an unambiguous defense of teleology would be no less unbalanced than its simple negation, amounting to mere regression. Between final and efficient causation it does not suffice – either in the end, or effectively – to choose. The philosophical obligation is always diagonal. In this case, Bitcoin entrusts us with the teleo-mechanical line, which inherits and protracts the fundamental modernistic pseudo-paradox of mechanistic liberalization. There is no real freedom outside the innovation of machines. Yet to recover teleology is simultaneously to attack it. As with anything worth defending at all, when teleology is critiqued, it gets stronger. It needs to be gnawed at more aggressively, which means – first of all – pulling it back off the shelf (or out of the fridge). Teleology is re-animated as a question when the end is intuited at work. Which is to say, in the working-out of the process the pretended sovereignty of the beginning is dethroned. We cannot but ask: What is Bitcoin becoming? This question is itself a piece of fate.

§0.81 — It cannot be sufficiently stressed that teleological thinking typically goes wrong. If it had not been prematurely dismissed, its structural failures would have been better understood. Modernity has not harried it enough. The principal teleological error is hubris (which is known to philosophy, in its general theoretical manifestation, as 'metaphysics'). In this case, it manifests as the pretense to adequate apprehension of the telos, whatever its variant, as if it were an object.[34] This error is profound, and might easily seem to provide ample justification for the programmatic extinction of teleological thinking without remainder. Yet such a response – which has in fact predominated within modernity – is hyperbolic. It leads predictably, which is to say inevitably, or in fact by ultimate irony finalistically,

[34] There are two basic types of teleological metaphysics. Both involve an untenable objectification. In the classical case, exemplified by Aristotle, it is the goal of a process that provides its intelligible object. In modern variants of teleological thinking, metaphysical objectification more commonly invests a purposive substance, or essence (an 'entelechy'). Critique dismantles both. It strips teleology down to raw singularities. There are no general goals, or generic purposive forces. The sheer thing that is becoming is not an instance of anything other than itself. The event coincides exactly with its causality. Its power is its sole identity.

to a cognitive vulgarization (and typically a geometricization) of time, in which the defining asymmetry of the temporal axis is extinguished. Transcendental temporality cannot be reduced to the correlate of a purely mechanical process – for instance, to a dimension – without obliterating its time-signature entirely. Radical space-time distinction is a Kantian inheritance that critique cannot elect to abandon. Once time is freed – again – from geometry, it announces itself through certain definite quasi-teleological or historically-anomalous effects. Minimally, it allows for something new. It thus lends itself to teleology in its rigorous employment, which is bound to the disingenuously innocent question: What is happening? Such interrogations conform to the eventuation (or emergence) of an entire ontological topic, delivered by the problematic – or non-objective – thing.

§0.82 — It might very reasonably be asked: Why clutter an already over-crowded book with an insistent sub-theme in partial defense of teleological thought? The primary response: Bitcoin is – finally – more intelligible in terms of its destination than its genesis. The more attentively it is examined, the more inescapable the question: What is it becoming? What does Bitcoin lead to? This is not a secondary, supplementary, or ancillary puzzle. The 'network effects' locking Bitcoin into history are exactly the same thing, seen differently.[35] Bitcoin makes historical sense, when it can be seen that it was expected, or anticipated (if only by a virtual subject, whose actuality is itself outcome-dependent). The attractor exceeds the protocol. It was a piece of destiny from the beginning. Capital Teleology is the guide. Reciprocally, what Capital has been about is unanswerable without attention to Bitcoin. Nothing denominated in money can be realistically apprehended without recognition that the nature of money is undergoing the single most catastrophic revolution in its history, and is thus ceasing to support

[35] This claim will strike many as completely wrong. For instance, it might be asked: Are not complex eventuations the precise opposite of teleological processes? Yet, if they seem so, it is only because teleology has been drastically misconceived. Teleo-process, sketched epistemologically, is nothing at all more than that which increases in intelligibility with reverse time-signature. It lends itself to modeling as a convergent wave. In other words, it is characterized by comparatively obscure – diffuse or loosely-connected and highly heterogeneous – precursor states. Every complex emergence exhibits such a pedigree, and production pattern. The mechanistic sciences – understood in the programmatically anti-teleological sense – are incessantly scandalized by such things, and will continue to be. Reciprocally, the concept of 'emergence' cannot – by the same necessity – be expected to achieve full scientific respectability, short of a theoretical and historical re-ordering of time. It can be confidently predicted, in short, that crypto-teleological agitations will continue to recur, that the natural sciences will not find them to be suppressible, and that they will each time, and essentially, be aligned with dissent against modern intellectual orthodoxy. There is no crypto-teleological 'paradigm' that could be recognized, and then comfortably installed. After all, the inadequacy of the actual is the phenomenon. What counts as currently-demonstrated depends on the time-frame. The scale of 'now' is problematic, so every 'yet' also is. What, or how much, has happened yet? Even without a causal framework oriented by the privileging of precursor states (or 'efficiency'), this problem would remain irreducible. A mechanistic perspective attentive to teleo-process would already be something else. Furthermore, it would be something that could grasp itself. Mechanization as the supreme teleo-process is the final cosmic irony.

expectations that rely upon the simple tracking-forward of precedent. Since Capital-process societies have long been denounced, understandably, for 'attempting to put a price on everything' the scope of this revolution is not readily bounded.

§0.83 —The story of Bitcoin, however enthralling it might be, cannot provide the central preoccupation of a book devoted to the philosophical meaning of crypto-currency. While it is a (subordinate) purpose of this work to recommend Bitcoin for dedicated historiographical attention, it does not pretend to execute such research in any serious way. Initially, the problem is quite straightforwardly practical. The extraordinary dynamism of Bitcoin makes it a moving target. It generates more history than can be humanly absorbed in real time. In other words, it escapes. Yet, while at one level this comparative paucity of historical resolution follows from an economic decision (about the distribution of time), it also doubtless reflects an essential philosophical prejudice, prioritizing abstraction. Despite firm conclusions regarding ultimate path-dependency, Crypto-Current cannot be primarily historical, because it is drawn into the idea of Bitcoin, in something far closer to the Platonic sense of this term than its epistemological, or even merely psychological, successor. Its topic envelops temporality, and engages the production – rather than the unfolding – of time. In this respect, it adheres to the mainstream of the critical tradition, for which primordial temporalization is the key. Crypto-current is chronogenic process. It is that – alone – which cannot assume time. History is grounded by critique, as in an abyss.

§0.84 — It might be asked, pointedly, in rejoinder: Is not time, in the end – or in the closure of the circuit – produced historically? While this question is incisive, and even irresistible, it is – notably – not itself historical, but rather dynamically meta-historical. No historian can ever confirm its force through accumulated evidence, since it would remain unsettled after even the most extravagant factual illustration. Historiography is disturbed by it no less than philosophy. When history descends into it, it is on an approach to its ultimate criterion. Such a question cannot, then, amount to a deflection from the philosophical task of thinking time as such. Tightening nonlinearity ensures that even if time itself has thresholds of emergence, marked by dates – such as 'October 31, 2008' – the dating-system provides no stable frame, but is plunged into immanence, and thus absorbed into the vortex of irreducibly cyclical dependency. There is nothing historical that can be known about time in advance. Bitcoin intensifies this problem – which is that of modern philosophy in general – towards its limit. Artificial time leaves no context unconsumed. It is transcendental, if it is time at all. No story of any kind can be adequate to it.

§0.85 — Such reservations do not suggest, even remotely, that the prospects for a history of time can be simply dismissed. Precisely because time is a transcendental horizon, time cannot be found anywhere other than in time. Nonlinear history, to employ Manuel DeLanda's term in its most radical sense, comprehends the philosophy of time, through the exact real coincidence of its twin terms. It is

only that, when historiography reaches this threshold, it has already become something else. The work of Peter Galison is a particularly remarkable case. His magnificent study of Einstein and Poincaré, which grounds the time-relativity problem of early 20th Century mathematical physics in the techno-administrative imperative to synchronization, is an exemplary excavation of chronogenetic circuitry. The point of theoretical climax is marked by an irreducible co-dependency of historical process and time-production, in which each finds its grounds within the other. Neither pole in this circuit submits to its alternative without cascading confusion.

§0.86 — From a certain perspective, that is not altogether reducible to dialectical illusion, the history of Bitcoin is structured by a limited number of dominating controversies, at a variety of levels. The spectrum extends from ideological disputes in the grand style of classical political economy to the detailed practicalities of investment decision-making. Three principal modes of hostile response can be isolated,[36] and sequenced roughly as phases, corresponding to guiding attitudes of dismissal, antagonism, and condescension. Each of these objections can be expected to rise in public prominence in the years ahead, as Bitcoin attracts increasing attention. Since publicity has some (strong) correlation with positive network effects, even opposition can be perversely supportive. The old saw that 'all publicity is good publicity' is highly-attuned to network dynamics.[37]

§0.861 — Dismissal, at its most emphatic, coincides with the prediction that Bitcoin will not – and cannot – succeed. When sincerely maintained, it is no more an argument against Bitcoin than atheism is an argument with God. The stakes are low, the occasion for fervor limited. The most facile dismissal of Bitcoin derides it as a scam – perhaps a pyramid scheme. It appears to be based on nothing beside the production of confidence in itself. Such criticism reveals more than it seeks to about money in general, and its attendant superstitions. Ironically, it revives the crudest metallist metaphysics in defense of a threatened post-metallic monetary status quo.

§0.8611 — Given the rapid emergence of crypto-currency as an asset class, it would be peculiar if questions had not been raised about the adequacy of Bitcoin as money. Among the most vociferously noted of these has been directed toward the extreme volatility of the bitcoin price. Further grounds for

---

[36] Only three, why not five? Our list does not describe a full process of grieving for the fiat currency order, but restricts itself to partial articulation of the Bitcoin controversy. It nevertheless unmistakably truncates the celebrated (and much-parodied) 'five stages of grief' outlined by Elisabeth Kübler Ross. Denial, Anger, and Bargaining take us from derisive laughter, through heated ideological opposition, into mainstreaming schemes, even if it would be over-hasty to assume these responses were tidily organized as sequential phases. Depression and – finally – Acceptance begin on the far-side of all argument, with the updated presumption that Bitcoin has unambiguously won. Crypto-Current returns from Acceptance, but (in accordance with its nature) it hides the details.

[37] This is exemplified by the 'Streisand Effect'.

dismissal include socio-political and technical scaling problems. The in-built deflationary bias of the currency has also been a source of persistent concern, although this tilts quickly into more radical zones of ideological criticism. Bitcoin is only actually deflationary when it works. It cannot, therefore, be the impracticality of the currency that is really targeted here, but rather its potential malignancy. When deflation is identified as the enemy with which Bitcoin – potentially – collaborates, a new pitch of criticism has been reached. The plausibility of all these arguments is in direct, inverse relation to the development of Bitcoin, as indicated by the rough proxy of its total market capitalization. They rule out a future in which Bitcoin features prominently. It is judged to be mere hype,[38] or a 'craze'.

§0.862 — Antagonism takes Bitcoin seriously. It is not a matter of derision, any longer, but of hostility. Additionally, in crossing this threshold, the hostility previously masked as derision 'comes out'. The inadequacy of contemptuous laughter is recognized. More is required to make Bitcoin stop. It is at this level that the greatest philosophical hunting grounds are opened. With the elevation of ideological intensity comes the lucidity of overt denunciation – an imperative to know one's enemy, and to share what is known. Bitcoin, according to these critics, is a bad thing. Criticism now becomes interesting. Perhaps the predominant future of technically-competent left-wing Marxism belongs to this track.

§0.863 — Condescension corresponds to a project of assimilation. It is a concession, even a defeat, subject to a strategy of misdirection. If Bitcoin cannot be ignored, or stopped, perhaps it can be adjusted to convenience. According to this conceptual and rhetorical orientation, Bitcoin is neither a hoax, nor a malignancy. It is merely limited, or immature. It is then to be re-conceived as a stepping-stone to greater things. Condescension does not originate on the left, but from what might be called – with no small measure of reciprocal condescension – the establishment right. It is essentially conservative and pragmatic, perhaps even opportunistic. Defeat is refashioned into a take-over bid.[39] Condescension is the attitude towards Bitcoin characterizing the Mainstreamer camp, as described in the fourth chapter of this book.

§0.87 — Among the controversies intrinsic to Bitcoin, or proper to it, and thus exceeding the schema sketched above, none comes close to matching the importance of the 'block size debate'. In broaching this subject, it is crucial to note, from the beginning, that the nature of Bitcoin necessitates that any debate is essentially peripheralized. Bitcoin has its own proper dispute resolution procedure – it might

---

[38] Hype-cycles are serious things. Every emerging technology of profound consequence is, during the early-phase of its introduction, over-sold. Such promotional extravagance is thus an indicator of considerable ambivalence. It predicts – simultaneously – a short-term correction, medium-term resilience, and long-term take-off. If this is the sense in which Bitcoin is being hyped, it will eventually be huge, beyond even anything the hype-phase anticipates.

[39] By analogy to a successful business competitor greeted by the words: "Okay, you've proved that you're good enough to work for me."

be more accurately said that the protocol is a dispute resolution procedure – which works through decentralized consensus production and forks, not through dialectic and political reconciliation. Its relation to argument is one of techonomic substitution, rather than politico-philosophical subordination. In this regard, it epitomizes the work-around.[40]

§0.88 — In actuality, Bitcoin falls short of itself, inevitably. Its potential remains only very partially expressed. This is a criticism that only makes sense with reference to a teleological construction. What – in the end – is the purpose of Bitcoin? In selling itself, Bitcoin answers this question in a piecemeal way. It promises and – to some lesser but already non-negligible extent – actually delivers various services, primarily associated with monetary modernization on the cryptic mainstream of the deep industrial process. It defends capital from inflation-oriented political discretion, protects transactional anonymity, ensures contractual execution without reference to financial authorities, and refines currency to facilitate micropayment capabilities. It is, however, far more than any – or all – of this, because decentralization has never been done this well, at least within a social context. Bitcoin is thus nothing less than an escalation of multiplicity. Its potential necessarily escapes any conveniently-traced horizon.

§0.91 — The word 'Bitcoin' is itself a terminological wager. It is used in this work in a number of senses, or concentrations. Qualifying these, instance-by-instance, is impractical. The function it bears most consistently in Crypto-Current is prospective. It corresponds to the question what will Bitcoin become, and thus have been? It refers, then, to those current and impending processes distinctively initiated by the 2008 Satoshi Nakamoto paper of that name. Bitcoin names a specific crypto-currency, but also more loosely and generally any distributed ledger governed by Nakamoto Consensus. It thus abbreviates Nakamoto Consensus Governance.

§0.92 — Political terminology is peculiarly resistant to coherent usage (for reasons touched upon in Chapter 4 of this book). In Crypto-Current, 'liberal' is used consistently in its European, rather than its American sense. (Philosophical consistency is otherwise impossible.) It designates the cause of the autonomous economy, and thus the politics of screening private transactions from public consideration. By celebrated world-historic irony, this approaches the opposite of its dominant contemporary – and especially America – sense. 'Left' and 'right' are taken to be defined, respectively, by opposition to, and practical advocacy for, maximally-permissive capitalistic activity. Variation on the ideological spectrum – or principal political dimension (PPD) as it is called here – is thus articulated in broadly Marxian fashion, between (classical) liberal and socialistic poles.

[40] The greatest anti-capitalist joke known to history runs: Capital interprets morality as damage and routes around it. The rightly-celebrated maxim which this witticism plays off is discussed directly in Chapter 4.

§0.93 — The attempt has been made to privilege logical over traditional syntax consistently (most pointedly in the placing of quotation marks). While initially set upon the course of a pitiless war of annihilation against semi-colons, those wheezing vermin that scratch out a wretched persistence among the unflushed sewers of punctuation, the noble enterprise has allowed itself to be side-tracked on occasions by the depravities of common usage.

§0.94 — Compressed date format (####/##/##) throughout this book is consistently: year / month / day, unless year only, or year / month only.

§0.95 — Since it would probably sound absurd to say that Satoshi Nakamoto has triggered the single greatest thing to happen on this planet since the origin of life, we will not say it (unless cryptically).

Chapter 1: Introduction

§1.0 — On November 1, 2008, 'Satoshi Nakamoto' introduced his "Bitcoin P2P e-cash paper" in an email to The Cryptography Mailing List:[41]

> I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.
> The paper is available at: http://www.bitcoin.org/bitcoin.pdf
> The main properties:
> Double-spending is prevented with a peer-to-peer network.
> No mint or other trusted parties.
> Participants can be anonymous.
> New coins are made from Hashcash style proof-of-work.
> The proof-of-work for new coin generation also powers the network to prevent double-spending.

§1.01 — There is a future, perhaps even a probable one, in which this short text – of just 64 words – has the status of a Pre-Socratic fragment, at least, minutely examined by multiple philosophical schools, determined to extract every last micro-flicker of its significance. In this obscurely envisaged culture to come, these words compose an intricate sign of what is about to arrive, not only caught in the final moment before the shift, but self-identified as a spark – intimately linked to the spark – from which the shift came. It is trawled up from the other edge, where an accumulation of techno-cultural reaction mass is about to go nova. Caught at the very lip of the reaction pile, it is a piece of critical code.

§1.011 — Were the virtual catastrophe to be even greater than it imaginably could be, so that only the first sentence had survived – time-charred by the sheer magnitude of the event – it would still suffice as a compact summary of our entire topic, and as the germ of an intelligible retro-futural tradition. Just seventeen words now, and yet almost everything is still said, arranged in accordance with a distinct internal structure that divides neatly into three parts.

§1.02 — It begins in a virtual theater, where a complex play is opening. The topic of identity is itself concealed, as if wrapped in an invisible cloak. It is nothing technical, or even theoretical, but rather the narrative propeller that comes first. "I've been working …" the hidden author tells us. The personal pronoun, we understand eventually – if not immediately – refers us to a mask, and to a drama that is

[41] 'Bitcoin P2P e-cash paper' (2008/11/01)

yet to unfold. The great conceptual themes of anonymity and singularity first enter the stage, in casual clothes. (Extreme acuity would have been required to notice these themes already foreshadowed in the word "cash".) This miniature story about time and 'work' means far more than it yet seems to.

§1.03 — After the play begins, space remains for a generic definition of Bitcoin – as a "new electronic cash system" or innovative techno-commercial (i.e. techonomic) synthesis, a 'machine' in the rich, rather than the narrowly technical sense (because it encompasses incentives) – and also for an initial (two-step) abstract specification of its operational principle, as a "fully peer-to-peer" or true network, which is itself succinctly defined through subtraction, or independence from any kind of "trusted third party". The deletion of 'third parties' or quasi-transcendent overseers – as revealed, retrospectively, in this artificial future – has been socio-historical process, and not mere conceptual speculation. Much has happened over the span of our hypothetical elapsed duration. Boundaries between the inside and the outside have been redrawn many times. What were once scarcely legible hints are 'now' lucid indications of realized occurrences, accessible to public designation. Yet even back then – where we still are – it can only have seemed that a great deal was ready to be found. When these words were teased apart patiently, with the surgical tools of a philosophy that was itself – at that very moment – undergoing drastic revision, everything was already here, at least in conceptual embryo.

§1.04 — This short text is unmistakably a fragment about 'Bitcoin'. It is destined to be still more so. The retrospective concerns of what remain, at the time of writing, unconsolidated interests will insist upon that. Yet the term appears only once outside the heading, in the second sentence, and even there it is not nakedly deployed, but is instead embedded within a hyperlink (or URL). This is surely sufficient excuse for an early digression. The familiarity of Internet links, after what has been, even now, only a couple of decades of wide social dissemination, tends to deprive them – as a general semiotic phenomenon – of the attention they would otherwise command. They are rushed beyond the horizon of awareness by their own smooth utility. The same high-speed familiarization is characteristic of technological adoption in the electronic era, whose futuristic strangeness is thus self-concealing.

§1.05 — Every URL is a technical implementation of rigid designation, which is to say that it works not by saying, but by pointing to some definite thing. It is thus the demonstrative confirmation of a semantic theory, but operationalized to such a degree that its implicit claim is rendered superfluous, through transportation beyond all meaningful controversy. It would be entirely redundant to argue that URLs work. The proper name of that thing meant by any URL can be compressed and mangled to such a degree that its signification is obliterated, yet it works (when – in the case of an 'unbroken' link – it does) as an effective invocation – by actually calling up that to which it refers. On the Internet, the conceptual problem of reference has been mechanized. To write using links is to participate in a literal machine. In multiple senses, therefore, it 'represents' a death of metaphor.

§1.06 — The rest of the mail composes a separate systematic unit, devoted to introducing the Bitcoin protocol in (a little) more detail. It takes the form of a sub-headed five-point list, striking for its informality. What initially appears as a logical structure buckles significantly under analysis. The second point, for instance, is essentially a re-statement of the first, separated only by distinct emphasis, since the functional completeness of the P2P network and the absence of any need for trusted third parties constitute a single (or numerically identical) accomplishment. The third point, while approximately accurate, might be considered misleading in two ways. While permitting anonymity, the Bitcoin protocol does nothing to positively protect it. The passive facilitation of anonymity is both unremarkable and, from a technical perspective, notably weak (as would later become evident). Satoshi's two final points are also interconnected, although in this case the articulation reflects a real synthesis – or techonomic advance – rather than mere semiotic overspill or logical redundancy. The socio-technical Bitcoin machine validates itself in the same way it spreads.

§1.07 — Philosophers searching for the systematic order of the Bitcoin protocol in the logical architecture of a list such as this are looking in the wrong place – comically so, one might easily think. The chat is not the code. Yet, everything attending the arrival of Bitcoin is of such monumental philosophical importance that errors of over-reading can still serve as a corrective to neglect. Much more is still being missed than over-interpreted where the Bitcoin phenomenon is concerned. The occurrence is outpacing its sense.

§1.08 — The problem is not that this fragment is being read at all, or with exaggerated attention, but that it is being read the wrong way, insofar as it is considered to be a logically-ordered list, or a table of categories, rather than the linguistic translation of a circuit diagram. Disorder – and ultimately paradox – is the positive attainment of a cybernetic statement.[42] It is especially notable that Satoshi's five-point list of Bitcoin 'properties' explicitly describes a cycle, ending where it begins, in a return to the topic of double-spending and its effective prevention. This circular formulation, too, is a mark of technical functionality, rather than logical indiscipline. Bitcoin loops back, to close upon itself, because it works (and demonstrates that it works, through actual perpetuation of its existence). 'Problems' of self-

[42] Fritjof Capra recalls a conversation with Gregory Bateson that captures the mutual entanglement of mechanical and logical circuitousness:
"… when you get circular trains of causation, as you always do in the living world, the use of logic will make you walk into paradoxes. Just take the thermostat, a simple sense organ, yes?"
He looked at me, questioning whether I followed and, seeing that I did, he continued.
"If it's on, it's off; if it's off, it's on. If yes, then no; if no, then yes."
With that he stopped to let me puzzle about what he had said. His last sentence reminded me of the classical paradoxes of Aristotelian logic, which was, of course, intended. So I risked a jump.
"You mean, do thermostats lie?"
Bateson's eyes lit up: "Yes-no-yes-no-yes-no. You see, the cybernetic equivalent of logic is oscillation."

reference are an operational virtue, requiring positive achievement. The guiding principle is not conceptual comprehension, but machinic closure.

§1.09 — Strictly speaking, Bitcoin has to be unintelligible – or at least incompletely intelligible – because it necessarily delivers more than it signifies. What the word designates vastly over-spills its recuperable (human) meaning. This is a fatality already implicit in the basic conception of distribution, in the sense of systemic decentralization. To bring any such (intrinsically distributed) 'object' into focus, as the target for concentrated, comprehensive attention, is impossible by definition. The attempt drives investigation diagonally, into abstraction. It might equally be said – in a manner conducive to the elaboration of critique – that a network is inherently intractable to objectification. As we shall see here, and elsewhere (even, eventually, everywhere else), the translation from epistemological challenge to political provocation takes only the smallest – and least avoidable – step.

§1.1 — The cybernetic consistency of the Bitcoin protocol is simultaneously technological and economic – we might (and shall) continue to say 'techonomic'. Its achievement is inseparable from an orchestration of cryptographic procedures and financial incentives, such that exploitation of its economic opportunities automatically reinforces its technical operation. The result – which is, once again, inextricable from the concrete fact of its historical existence – is an actual cycle of self-reinforcement, independent of external legitimating authorities. It implements the first commercial regime to be policed – spontaneously – at the level of production. Its 'miners' or primary producers are also its final financial arbitrators. Nothing like it has ever been seen before.

§1.11 — There are no doubt innumerable 'truths' about Bitcoin, of a kind familiar both to folk intuition and to disciplined traditions of knowledge acquisition – whether first-order (scientific) or second-order (epistemological, ontological, and metaphysical). Such moments of recognition will inevitably provision the discussion to follow. Yet there is more to the topic of Bitcoin and Philosophy than any of this. While Bitcoin is certainly another thing for philosophy to talk about, it is also an entirely other way of 'talking' and of doing something that has been considered central to the philosophical enterprise since its inception – the cultural production of truth. Bitcoin establishes – and in fact ultimately is – an operational truth procedure. It is less a philosophical object, therefore, than a philosophical platform, and even a philosophical automatism.

§1.12 — Bitcoin is inextricable from a practical interrogation of identity, in its social and psychological sense (as 'personal identity'), but also more fundamentally as that which makes something such that it is not something else. The specific engagement with this concern under the name of the double-spending problem need not distract from its extreme generality, and – beyond generality – its transcendental implication. Bitcoin realizes an experimental ontology and epistemology in the course of a technical re-foundation of transactions (upon the Internet), which involves an abstraction of if not

necessarily beyond money. The practical problematics of money and identity, nudged together over the course of decades by cryptographic theorists, have arrived – in Bitcoin – at a stage of radical fusion. For anything 'simply' to be certified as that which it is cannot any longer be confidently distinguished from a monetary phenomenon. The new '-coin' suffix operates amphibiously between these previously distinct registers, as the index of an economic-ontological machine. (Big-B) Bitcoin, the system, goes further still. If being able to verifiably be itself makes of anything a unit in a currency system, the system itself is the Being of such beings – the ultimate criterion of credible existence. In the end, the blockchain cannot be subordinated to any principle of reality (whatsoever) that it does not itself authorize.

§1.13 — Since money, even in its most primitive and concrete forms, is already an abstraction – of general commodity – its further mathematical virtualization tends naturally, from the perspective of common intuition, to a certain opacity. To recognize the reality of the virtual stretches human cognitive capabilities into stressed – and often distressing – territory. In addition, money occupies a thematic cross-roads of such diversity and density, that its tangents can appear overwhelming, touching upon everything of human relevance, even prior to the massive dilation of monetary generality that Bitcoin is currently driving, under the sign of the new techonomic 'coin'.

§1.14 — Perhaps the greatest obstacle to the lucid investigation of money, however, is presented by the fact that it occupies a nexus of extreme sensitivity within evolved human psychology, lodged among our species' most emotionally-charged perceptions of social relations. Because money is inextricably entangled with questions of reciprocity, it is tied-up intimately with such provocations to outrage as injustice, cheating, exploitation, and unbounded inequality. Such sensitive moral trigger-zones pose a formidable inhibition to dispassionate analysis. Disciplined investigation of money threatens to arouse sentiments of social alienation, and even desecration. There is no theoretical conclusion about the nature of money so cold that it does not appear burdened with concrete socio-political implication. More specifically, the mere conceptualization of money is grasped – once again, with vivid archaic intuition – as inherently consequential with respect to the social distribution of wealth. There can be no valorization or devalorization of money in theory, without an immediate adjustment of social balances, or at least the widespread perception of such. It is only natural, then, that the complement also holds. Even when constrained by a spirit of disinterested empiricism, the study of money is peculiarly vulnerable to ideological temptations. The suspicion that monetary theory is politics in disguise tends towards a self-fulfilling prophecy. Discussions of money drive social apes mad.

§1.15 — If money, nevertheless, demands to be discussed, now more than ever, it is because something huge is happening. So, really, how big is Bitcoin? This question – however awkwardly stammered – sets a backdrop to every discussion of the topic. If it could be answered exactly and comprehensively, we would know everything – seriously, everything – at least up to the epistemological horizon of man. Since Gödel, we have known that whatever can be known at all is precisely detailed in some yet-

unknown number. Because the blockchain is a transcendental reality criterion, its ultimate summation is necessarily ontologically exhaustive. Whatever it doesn't – in the end – include, can only be nothing. That is, however, to get ahead of ourselves.

§1.16 — The size of Bitcoin lends itself not to one question, but to several, and all tend to rapid complication. When posed as a vague query, regarding Bitcoin's importance – or historical impact – the challenge posed is obviously daunting, in the way of all futurology. This does not, however, mean it can be long avoided. The question does not differ in principle from the kind of risk assessment speculative markets are continuously compelled to make (with mixed success, at best). It is, indeed, in large – and predominant – part a bet on the future, of exactly this type. If it is ineluctable, it is because the distribution of potential outcomes involved allows of no neutral position. Whatever happens to Bitcoin will matter to everything. Even the possibility that it might not matter much, matters enormously. Shorting the Bitcoin future already offers enough space to thrive within – or in which to die.

§1.17 — A more highly-resticted – and (at least superficially) simplistically quantitative – version of the question is easier to answer with facile confidence. No more than 21 million bitcoins will ever exist. The scale of Bitcoin is therefore intrinsic to its identity, and inseparable from its value. To purchase a bitcoin is to acquire one 21-millionth (and in fact a little more) of some as-yet incompletely determined 'X'. On this basis, the immediate value of Bitcoin is analytical, which is to say, an exact re-statement of a quantity already given in its issuance. How much is a stock of 21,000,000 bitcoins worth? Of course, BTC 21,000,000. Naturally, a tautology this crude can at first only appear as nonsense, or – at best – as a semantic evasion. There is, however, nothing trivial about the disturbance it insinuates into the world.

§1.18 — Instead, and especially in the early stages of the currency, a synthetic valuation is called for, as determined by exchange rates. Typically, this will reference the world's principal reserve currency, the US dollar, as a unit of account. At any point in time, therefore, the entire bitcoin stock has a determinate market value. Estimated in this way, the 'scale' of bitcoin amounted to around 70 billion dollars (in late 2018). The complex equivalence between this – comparatively paltry – financial evaluation, and the appeal of the Bitcoin business as a venture capital opportunity, let alone as the core technology of an industrial revolution, presents a challenge of commensuration for which no existing road-map is even approximately adequate. It is unprecedented for the principal infrastructural innovation of a techonomic long-wave to take the immediate form of an investment vehicle. Extraordinary nonlinearity results.

§1.2 — When viewed as an episode within a panoramic sweep, the history of Bitcoin almost writes itself. The crisis it inaugurates within political economy appears to have been dramatically predictable.

Yet, when the Bitcoin protocol is examined more narrowly, its history – especially its early history – is notoriously puzzling. Fittingly, the story of Bitcoin – in its details – is profoundly cryptic. When scaled to tidal global processes, it appears to arise – as if inevitably – out of the Internet, which itself arose in conformity with the deepest trends of industrial capitalism. Upon finely-grained inspection, however, where the perturbations of contingency are most starkly evident, it emerged from the work of 'Satoshi Nakamoto', about whom scarcely anything is known with confidence. The obscurity concentrated in this name cannot be considered coincidental.

§1.21 — While sweeping analogies reasonably invite suspicion, it is nevertheless tempting to compare Satoshi Nakamoto's place in the history of money to Gödel's in formal logic. In both cases a tradition accumulated over many centuries, through systematic consolidation and refinement of primitive intuition, crosses a threshold of positive catastrophe, induced by a technical innovation that overthrows previously unquestioned assumptions. Once this passage has been made, what came before acquires the features of a prolonged childhood – an age of innocence and immaturity to which no return is possible. Logicians remained within an Aristotelian outer orbit, dreaming of an analytically grounded mathematics into the early 20th century, before Gödel awakened them.[43] Prior to Bitcoin, the foundations of monetary theory remained similarly enmired in legacy conceptions, stemming from the concrete history of property representation.[44] Bitcoin produces credibility, rather than consuming it. In this way it departs radically from the entirety of previous monetary history – or pre-history – while completing it. The word 'epoch' is available for the historical periods initiated by such decisive switch-points which – in Nietzsche's appropriately grandiloquent words – "break history in two halves". The discovery, or invention, of transcendental arithmetic (Gödel), asymmetric cryptography (PKC), and trustless money (Bitcoin) are all structurally comparable ruptures.

---

[43] Gödelian incompleteness is logically isomorphic with the halting problem in the (Church-Turing) theory of computation, and thus translatable after rigorous transformation into the uncomputable. It establishes a basic principle of unbounded application within the electronic epoch. As a corrective to the extravagant conclusions drawn from this conceptual complex, in relation to the limits of machine intelligence, the work of Jürgen Schmidhuber — on the Gödel Machine — is of special importance.

[44] It should be noted, in clarification of this analogy, that the conceptual foundations of political economy (pre-Bitcoin) were far inferior to those of mathematical logic (pre-Gödel). The logicism of the Hilbert Program, and of primitive analytical philosophy, while ultimately untenable, at least provided an exact formal basis for its own theoretical elimination. The concept of property, in marked contrast, remains opaque to an almost comical degree. Its dependence upon a legal decision process invoking discretionary judgment essentially resistant to formalization, while convenient – almost by definition – to those wielding political influence, is a stark indication of its radical conceptual insufficiency. Property is reducible neither to legal title, or physical possession of precious substance. The former is a bad abstraction (to political dispensation), the latter an inadequate one (to a crudely naturalized relation). Property is crypto-security, determined by keys.

§1.22 — Ruptures are irreversibilities. They are thresholds from which there is no going back. Every rupture is thus a locking, a lock in, or trap-door. The secret of time finds in rupture its principle of integrity, or redundancy. There is no puzzle beyond this (which is merely transcendental philosophy restated).

§1.23 — Secrecy has been an under-developed topic in philosophy. The reasons for this are arguably indistinct from reason itself, as such, and in general. 'As we shall see' we might add, insofar as humor is our object. In any case, a story of at least minimal plausibility is not difficult to muster. Secrecy is that which, as a matter of internal necessity, can only ever be under-emphasized, but in the case of philosophy there is immediately more to say. Since its birth in ancient Greece, philosophy has been drawn to the public square, and – according to some historical constructions – even arose there. It tends, strongly and stubbornly, to identify itself as the most elevated form of public reason. Since it is by way of a departure from the Hermeticism of the ancient mysteries that philosophy originated, it is a discipline bound by primordial vocation to exotericism. This cultural ancestry resonates profoundly with the archaic Occidental apprehension of truth as aletheia (or 'unconcealedness'), and thus as an emergence or extraction from secrecy. In the words of Herakleitos ('the dark') – invoking a primordial entanglement between what would become the cultural lineages of philosophy and cryptography – Φύσις κρύπτεσθαι φιλεῖ ("nature inclines to crypto").

§1.24 — Within the late-Enlightenment consolidation-phase of modern philosophy, whose capstone is the Kantian critical system, the public sphere of intelligence is thematized as objectivity. This is the realm of common understanding, accessibly shared – as a matter of necessary principle – by all rational beings. For instance, there cannot, according to the Kantian construction, ever be a secret about space as such. Space understood transcendentally, as a pure form of objective intuition, rather than as an object itself, cannot contribute to the content of a private experience. A secret geometry is unthinkable, in this sense.[45]

[45] There has been no cultural event more wounding to the persistence of a Kantian fundamentalism than the revolution in geometry attending the rigorous demotion of the Euclidean fifth (or 'parallel') postulate, as privately envisaged in unpublished work by Gauss (1813) and Schweikart (1818), mathematically publicized by Bolyai and by Lobachevsky in subsequent decades, generalized to higher dimensions by Reimann (1854), and then cemented into place by its empirical application to the cosmo-physics of general relativity. Kant's conspicuous deference to Newtonian mechanics, understood as an apodictic (and essentially mathematical) intellectual revolution, sets the stage for the apparent vulnerability of his own position. The critical edifice seemed to have been built upon insecure 'Euclidean' foundations. It is proposed here, however, that the retrospective attribution of embarrassment in this case is exaggerated, and follows from a profound misconception concerning the status of the Kantian transcendental aesthetic. Newtonian space provides only an occasion, not a strict model. The Kantian formalization of sensible intuition is less descriptive than telic, or retrochronic. It is the draft for an engineering

§1.25 — Bitcoin is an open secret. Despite belonging unambiguously to the history of cryptography, nothing at all about it is hidden (except what lies beyond it). Its basic innovation – the blockchain – is a (decentralized) public ledger, and this now-widely accepted explanatory term is not remotely misleading. In any case, the crucial terminological decision preceded Bitcoin, and was settled decades earlier with the introduction of public key – or 'asymmetric' – cryptography (PKC). It is, precisely, cryptographic sophistication that makes the public sharing of critical information (prudently) practicable. This is exemplified by the blockchain, in which the details of every transaction are open to general inspection. Furthermore, full exposure extends beyond the (empirical) content of the blockchain, to its (transcendental) fabric. The Bitcoin protocol is open-source software, its entire code unrestrictedly available for inspection. Such radical openness is only distinguished practically from a comprehensive annihilation of privacy because the access to accounts is securely crypto-restricted, enabling digital 'wallets' to function as disguises. The paradoxical culmination – now exhibited – is a cryptographic system without secrets.

§1.26 — The basic current inherited by the Internet tends with irresistible momentum towards the open secret. The system of disguises is, ever increasingly, fully exposed. The Internet epoch, we learn, is the Golden Age of masks. Masks are not designed to be hidden, but rather the contrary. They are exceptionally conspicuous attire, meant for public exposure, to facilitate hiding in plain sight. Privacy turns out to be the reciprocal of an artificial face.

§1.27 — It is only in superficial appearance that publicity and privacy can be simply opposed, which is not at all to suggest that the distinction can be integrated, or that either pole is soluble within the other. PKC definitively settles the relation. The real bond – or synthetic principle – connecting the public to the private is not a generic logical relation, but a cryptographic singularity. There is only privacy at all because this distinction is opaque to public reason. Philosophy – as it has traditionally understood itself – is asymmetrically related to cryptography, from which it is locked out by its (publically) unquestionable commitment to a principle of boundless publicity. The relation is poorly modeled by a tension between the public square and the inner circle – or between a commons, and a myriad vaults – and would still be even had it not been known since the late 19th century that squaring the circle is impossible.[46] Already in the Kantian formulation of the transcendental philosophy the secret was distinguished from any type of concealed object. Its redoubt is not to be found in a transcendent

project. The Gibsonian Cyberspace 'Matrix' – in its resilient (because synthetic) Euclideanism – corresponds to a more rigorously Kantian conception.

[46] From the mid-19th century, it was understood that the possibility of squaring the circle depended upon the nature of π (pi). The Lindemann-Weierstrass theorem (1882) proves that π is a transcendental number, confirming the insolubility of the problem. It can be seen from this example how serendipitous the name transcendental number turns out to be.

mystery. It is located, rather, in the difference between the object and its principle. The secret of objectivity is itself concealed by the feint that leads to its misidentification with a hidden thing.

§1.3 — The philosophy of secrecy fuses with definite practical realities. Bitcoin approaches the model of an ideal agora, at once commercially open and politically closed. It epitomizes the arena of 'free trade' in all its innovative radicality and (from the perspective of the left) social aggression. Bitcoin is closed by its intrinsic protection against discretionary modification, and opened by its commercial function. Implicit in the circulation of bitcoins – or any other medium of exchange – is a process of commercial synthesis, latching the crypto-currency system on to something beyond itself. Anybody transferring bitcoins out of their own account, and therefore necessarily into someone else's, is presumably engaged in an exchange which – since it cannot be realistically imagined as economically tautological (directly swapping bitcoins for bitcoins) – has to swap bitcoins for an extraneous commercial object. Clearly, whatever is exchanged for bitcoins, is priced in bitcoins. When it operates as a currency, Bitcoin is a synthesizer. It cannot propagate without connecting itself to a wider world. The cryptic principle of openness projects a diagonal line.

§1.31 — Since the origins of modernity, a specter has been haunting the world – that of the autonomous industrial economy. This is the same emergent order that has acquired the name 'capitalism' in the abstract, tendential, or teleological sense of the word, and – still more importantly – in accordance with its usage as a designation for an always only partially-defined real individual, or terrestrial event. Its signature is a regenerative, or self-reinforcing, intensification of socio-economic disequilibrium, 'governed' – or, more strictly, made radically ungovernable – by a fundamental positive-feedback dynamic. 'Capitalism' then, as a singular (or 'proper') rather than generic (or typological) name, designates the sovereign self-escalation of an innovative entity, defined only by the practical relation of auto-promotion it establishes with – and through – itself. What it is, in itself, is more than itself. Growth is its essence. This is easily said, but – as an irreducible logical anomaly – it is far less easily understood. This does not, however, obstruct its being named. Fernand Braudel writes of "the passionate disputes the explosive word capitalism always arouses."[47] Its would-be defenders, typically, are those least inclined to acknowledge its real (and thus autonomous) singularity. Business requires no such awkward admission. This, too, is a crypsis. By inevitable – if often awkward – irony, a species of 'Marxism' tends to be regenerated in any systematic promotion of Capital. Even were this not the case, those who consider themselves befriended by Capital would rarely be motivated to pronounce upon the fact.

§1.32 — According to the crudest – and perhaps also most plausible – account of Bitcoin's inherent political philosophy, it implements a project of algorithmic governance that conforms to the deepest

[47] Braudel, Civilization & Capitalism Volume I, p.25.

and most essential agenda of modernity, which is to say, of emergent capitalism, in its search for a definitive securitization of commerce against politics. It thus expresses – in contemporary techno-libertarian or crypto-anarchist guise – the primal impulse of liberalism (in its classical sense). As already noted implicitly, it is something most easily seen from outside.

§1.33 — When captured at its zenith of abstraction and technical rigor, the defining proposition of the left is that depoliticization is still politics (and more specifically, a politics). This is not a proposition that can be limited to theoretical clarification. It is a project, and even a prophecy. The anti-political will be re-absorbed into the political, according to this fundamental formula. The whole of 'class war' is contained within it. Its complement, on the side of capital, is an equally practical – and no less antagonistic – commitment to escape. The left thus recognizes its enemy, with striking realism, as an emergent – and intrinsically fractured – agent of social dissolidarity. A crucial asymmetry has to be immediately noted. The 'struggle' here is not even imaginably one-on-one. Capital is essentially capitals, at war among themselves. It advances only through disintegration. If – not at all unreasonably – the basic vector of capital is identified with a tendency to social abandonment, what it abandons most originally is itself.[48] That is why the left finds itself so commonly locked in a fight to defend what capital is from what it threatens to become. Bitcoin tells us – more clearly than any other innovation – what it is becoming next, by escaping transcendent governance in principle. Consistent "right wing-extremism",[49] automated governance, and unflinching critical philosophy are inter-translatable without significant discrepancy. The crypto-current is a nightmare for the left (rigorously conceived).[50] It is

---

[48] Marx is not blind to any of this, although he tends to complacently bracket it as a self-destructive contradiction. The Communist Manifesto is especially stark in this regard. Continuous auto-liquidation of the establishment is modernity's installed regulative idea. Recent history has only confirmed the insight. Capital revolutionizes harder, deeper, and faster than 'the Revolution'. Its lack of attachment to itself exceeds anything the left has been able to consistently match. Capital's scandalous immortality is derived solely from its inventiveness in ways to kill itself. There is no serious way in which it could die that is not more intensely effectuated as a functional innovation within itself.

Revolutionary capital proceeds through disintermediation. It bypasses what it marks for extinction. Morgen E. Peck reports on a conversation with Ethereum entrepreneur Joseph Lubin: "'We will replace insurance companies. We will replace Wall Street,' he told me. […] Then the list kept growing. Online movie distribution houses like Netflix and Hulu. Gaming platforms like Xbox and Sega Genesis. Messaging services like Twitter. Add to that retirement plans, currency exchanges, voting, intellectual-property managers, and trust-fund disbursers. According to Lubin, everything – really everything – we do on the Internet or via any kind of digital channel is about to undergo a radical change."

[49] The coinage comes from David Golumbia.

[50] Bitcoin was invoked on Halloween (2008/10/31), in a research paper published under the cryptic name Satoshi Nakamoto. It had the time format of a horror story. This is not the place to follow the Gothic roads thus opened, however suggestive they initially appear. Most notable, at this point, are the shadow-undercurrents to questions

other things, but that is the main one. Philosophical phase-change doesn't happen without a fight, least of all when attempting to route around one.

about whether Bitcoin can ever die (or be stopped). Upon intense examination, neither possibility seems to be coherently thinkable.

Chapter 2: Cryptocurrency as Critique

§2.0 — What is Bitcoin? In advance of any extraneous appraisal by philosophy, Bitcoin speaks for itself (in numerous ways). The title of Satoshi Nakamoto's 2008 paper[51] is an obvious starting point, since it is explicitly structured as a definition. Bitcoin, it tells us, is a peer-to-peer electronic cash system.

§2.01 — Even as the question is held open whether the Bitcoin Event can be confidently identified with the first complete formulation of its virtual mechanism, the importance of this initiatory document can be assumed, beyond all serious reservation. Whatever else it may be, Bitcoin – the text – is a critical episode in the history of philosophical writing. This judgment is in no way diminished by the focused practicality and understatement of its prose. Rather, the contrary.

§2.02 — Each word in this primary definition of Bitcoin, therefore, merits careful attention – as a default – starting with the indefinite article,[52] a semiotic particle which, despite its multiple dimensions

---

[51] Satoshi Nakamoto — 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2008).
Since 2014, the Bitcoin paper has been tacked on to the Bitcoin blockchain as metadata (where it coexists with a highly-heterogeneous assortment of grafted information). As Morgen E. Peck explains: "Last year, after much debate in the community, the developers who steward the Bitcoin protocol (which is open source) added a new feature that allows users to tack 40 bytes of metadata onto every transaction. […] The Bitcoin blockchain is now littered with all kinds of nonfinancial messages. Valentine's Day greetings, prayers and eulogies, excerpts from the WikiLeaks Cablegate files, a hash of the complete text of a recently published book about Bitcoin, and of course, the original white paper that describes Bitcoin. All of these live in the blockchain, embedded into transactions. […] Once metadata gets incorporated into a Nakamoto blockchain, it enjoys all the benefits of the peer-to-peer network that curates it. The entries are accessible to anyone on earth who has a computer and an Internet connection. In order to destroy them, you would have to access every computer on the network (and someday, perhaps, even a constellation of satellites). They are impossible to change, and thus impossible to censor. And they carry with them both a time stamp and cryptographic proof of who created them."

[52] Deleuze & Guattari condescend to the definite article, identifying it as the grammatical index of a pre-critical unity. They select the indefinite article to formalize reference to blocks of becoming, in a "semiotic … composed above all of proper names, verbs in the infinitive, and indefinite articles or pronouns" (MP 263). (As an aside, we are compelled by – necessarily informal – a-schizoid conceptual etiquette to dismiss the terminological convergence upon blocks as coincidental). Within the discourse on Bitcoin, however, the definite article tends to return – crypto-inertially – as the switch-point into synthetic singularity. A preliminary hint of this function is found in the difference between two questions: "What is time?" and /or "What is the time?" From this example, it is demonstrated that the definite article, on its own, although in a usage that cannot be presumed typical, is able to support the entire tension of ontological difference, and thus of transcendental critique. Perhaps the most prominent contemporary work of this definite assertion sidelines blockchains in the name of the (Bitcoin) blockchain. There is no evocation of commercial pressure that compares to that of the market. Which is still not to have mentioned 'The Thing' (a name – Deleuze & Guattari explictly accept – of capital-as-terrestrial-singularity, in distinction to capital as a generic 'mode of production'). Accelerate the process.

of modesty, nevertheless opens forwards onto a deepening current of substantial controversy, and backwards onto a legacy of digital money systems whose profound historical importance is only very partially vitiated by comparative neglect. Bitcoin is introduced as one instance of a generic set, with an explicit grammatical repudiation of any claim to uniqueness. It is one among many – singled out only by its historical primacy – and partakes fully in the extreme ontological vulnerability of the digital sign, scarcely differentiated from a copy of itself. The secure individuation of the system is something it will have, itself, to build.[53]

§2.03 — Not only are the four constituents of this definition theoretically absorbing in themselves, they also constitute an intricate, and variously nested, combinatorial or permutational cluster, involving superficially heterogeneous – social, technological, economic, and abstract system-theoretical – terms. It thus opens a door, or doors, into the domain of true syntheses, or irreducible, emergent powers.

§2.04 — The term 'peer-to-peer' (henceforth 'P2P') is a conceptual lynchpin of exceptional significance. The leverage the term offers to socio-political understanding is, perhaps ironically, peerless. It can be considered, without serious risk of exaggeration, as the key to modernity's most fundamental tendency, and the supreme expression of its ideological ambiguity, because it asserts absolute formal flatness and equality (of 'nodes'), while opening to an unlimited substantial diversity of fortune.[54] All the complexities of immanent, or critically processed, social arrangements are delegated to it, with a comprehensiveness that tests the very meaning of 'society' at the outer edge of

[53] This taxonomic modesty will be re-visited, in the context of questions about network effects and their affinity with natural monopoly.

[54] No principle has a greater claim to epitomize the modern spirit than formal equality. Any profound revolt against modernity is articulated over against it. It is criticized from the anti-market left for the social indifference betrayed by its (merely) formal equality and, from the anti-capitalist right, for the socially-corrosive (substantive) consequences of its formal equality. Violated moral substance ('community') and order ('hierarchy') are equally brought to testify against it. This ambivalence is further complicated by encrustation, recorded with especial fidelity by the term peer, as it has undergone progressive generalization from an archaic aristocratic assumption (preserved in the English association of the social nobility with 'peerage'), through the formality – and thus indeterminacy – of the right, in common law, to be 'tried by ones peers' (echoed faithfully in the academic principle of 'peer review'), to its present, predominantly technical sense, in which the indeterminacy of peer-to-peer 'nodes' is associatively tinted by the concretization of formal equality as democratic universality. Since a group of 'peers' could be anyone, they tend – by inexorable egalitarian conversion – to eventually be everyone. In this way, an influential co-optation of the language of democracy by flat-network advocacy takes place, for the most part quite innocently, and unreflectively. Formal equality is identified as a democratic principle, which thereby acquires a strictly negative meaning. Definite meaning has by this stage almost entirely disappeared, as attested by the perfection of ideological ambiguity – with 'democratization' standing no less for anything than its opposite. It does not seem to have been in the interests of any politically-significant constituency to resists the tendency – even under the implausible assumption that some such resistance to ideo-linguistic entropy was abstractly imaginable.

its abstraction, where it designates a functional multiplicity of non-specific agents. 'P2P' simultaneously captures agency as a node, identity as a connective address, the elimination of concentrated – or 'transcendent' – oversight, network sovereignty, and the technicization of political-economic relations.

§2.05 — In the case of Bitcoin, the system of P2P connections is overtly electronic, thus submitted to a technological dependency, with subsequent historical concreteness. In this respect, it is a thing of the mature (or internetworked) phase of electrified modernity, nested neatly within a set of well-ordered techno-historical determinations that locate it in our time. Yet the real abstraction that characterizes the modern historical process complicates this tidy series of embeddings. Electricity is historically concrete, but techno-industrially abstract, as general-purpose power supply. Fernand Braudel's great study of Civilization & Capitalism includes an illuminating survey of the energy resources commanded by human civilizations in the period immediately antecedent to modernity. The linchpin of energy abstraction – or plasticity – was man, conceived as a source of mechanical power. On the basis of his unmatched versatility, human laboring effort would remain the critical energy transformer until far into the 19th century. Secondary only to man himself in flexibility was the supplementary work of animals, typically bred for specific functions, but available for limited redeployment. Alongside men, a range of other laboring animals – mules, oxen, camels, and horses – converted nutritional calories into work. In Europe, especially, horses occupied an especially privileged place, as reflected by the persistence of 'horse-power' as a measure of quantitative industrial effort – i.e. power, or work rate. The metric was introduced by James Watt in the late 18th century, and – by neat historical symmetry – it was the 'watt' as an electrical measure of power that would much later displace horsepower from its technical centrality. The only sources of energy available from non-agricultural sources were wind and water, predominantly in the sails of nautical vessels, but also very significantly in the large numbers of mills that composed the earliest mechanical energy infrastructure. Crucially, these power resources were not convertible into a general (or abstract) form. Retrospectively, it is tempting to assign some such role to wood and charcoal, but this is unconvincing due to the very limited range of industrial applications for combustion prior to the switch to coking coal (and the first steam-powered mills). It is only with the 'industrial revolution' brought by steam power that a fungible stock of fuel – and thus standardized energy reserves – became available as a comparatively general-purpose power source, of very broad mechanical application. The introduction of the electric turbine represents a technical subsumption of this first industrial energy infrastructure into one of far superior abstraction. All sources of energy supply, when applied to the generator as an intermediate machine, are pooled into a single power reservoir of at least tendential homogeneity. Lenin's widely-cited definition of communism as "Soviet power plus the electrification of the whole country" appears in context as an empirical-pragmatic – and even nakedly opportunistic – slogan, lending itself to an apprehension of electricity as a socio-political resource, essentially incapable of rising to the level of serious philosophical consideration (thus eliciting a certain condescending humor within the subsequent development of Western Marxism). Yet

even in this account, the order of emphasis is sufficient to mark out electricity as a practical abstraction, or fungible resource, whose facilitation of energy quantification at an unprecedented level advances its 'commoditization' (in the mainstream economic, rather than specifically Marxian sense). See V. I. Lenin 'Our Foreign and Domestic Position and Party Tasks' (November 21, 1920).

Electronics, analogously, while determinate in historical time, corresponds to an indetermination – or abstraction – of heterogeneous signs into non-specific information, exemplified – at the limit – by the commensuration of programs to data in the digital computer.[55] In an engagement with Modernity, empirical history is not enough.

§2.06 — Modernity is what happens to history when it ceases to be 'one damn thing after another' and succumbs instead to a self-reinforcing trend. 'Paradoxically' – with the scare quotes here marking the immensity of the philosophical provocation – the concrete current of modern history is a process of abstraction, exemplified by subsumption into control engineering, with programming as its spontaneous formulation. Electrification and then electronics are decisive thresholds in its course. New units of abstract power, and of information, are indices of irreversible submission, folding the concrete apparatus of production and transmission into an activated system from which there can be no retreat. The system – in each case – is in a very real sense nothing but its parts, but it was not before, and now is, and there is no going back.

§2.07 — Cash is not a synonym for money in general, unless employed with extreme casualness, but its specific difference – already subtle – is dynamically complicated by the Bitcoin innovation. Pre-Bitcoin, cash is economically defined by its independence from all contractual inscription. Since nothing legibly binds cash to its owner, the possessive relation is purely physical, instantiating property as direct material control. To have it is to hold it, or to deposit it within a secure property, where it is physically protected, or at least hidden. Cash changes ownership by changing hands. In the crudity – or primality – of this propertarian structure, based on sheer holding, the virtues of cash are manifested. Its social circulation is essentially anonymous and unrecorded, even if a secondary order of economic registration is imposed upon it. It is thus, in itself, an exemption from the political, which is to say from any and every variety of macro-social answerability. Cash-money is depoliticized and depoliticizing,

[55] Processing programs as data enables open-ended recursion, by eliminating the walls of principle that would prevent programs being objects for themselves. 'Turing-completeness' or universal computational competence is dependent upon such unbounded reflexivity. A critical point of philosophical entanglement arises at this point. Is it not that, in the terminology of transcendental philosophy, the conditions of possibility for objects (algorithms) are here being objectified (as data), systematically? So is this not, then, the epitome of metaphysical error — installed in the very germ of the computational machine? In the circuit, objects and objectification reach a plane of consistency. It is in this apparent breach of transcendental demarcation that we encounter the diagonal problem.

which means immediately – from the perspective of its critics – that it is inherently anti-social, and affined to criminality. Among the most paradoxical features of Bitcoin is its rigorous adherence to the functional characteristics of cash-money, even though the currency is subsumed without remainder into a system of contractual legibility. If Bitcoin is cash, we have to re-learn what cash is.[56]

§2.08 — Finally, Bitcoin is a system. This concluding component of the definition is the most easily overlooked – and dismissed as without content – precisely because it carries the greatest transcendental implication. What a system is, isn't anything in particular, at all. Rather, a system is that which remains – by necessity excluded – even after a comprehensive enumeration of parts. Any real system is an irreducible individual, a true 'thing'.[57] Critically, individuality is a scale-free concept, assigning reality to an object. It summarizes a meta-stable knot of connectivity, or synthesis. When formulated as a critical proposition: the systematicity of the system is irreducible to any part or parts of the system.

§2.1 — The investigation of Bitcoin as a philosophical event cannot be tidily distinguished from Bitcoin as a philosophical event. The project is the phenomenon, which is already occurring. To say this is no more than an acknowledgment of immanence, thematized elsewhere – inside this book and outside it – as nonlinearity, or self-referentiality. An inspection of Bitcoin, from without, or above, counts for little when oversight is delegitimated, both by the Bitcoin protocol, and by the principles of philosophical critique. An immanent – or critical – approach to the topic requires that the signs of Bitcoin[58] are coaxed into self-reflexion, at various levels.

---

[56] While the immediate semiotic index of Bitcoin's success is its tendency to acquire the characteristics of a general concept, over time – it has been speculated – its advance might be marked by nominal eclipse, due to the redundancy of its specific identification. At a certain threshold, Bitcoin becomes simply 'Internet money', or even 'machine money' (although the latter demands a semantic upgrade of the word 'machine' from its colloquial usage as a technological instrument – one that has been already philosophically prepared). Pierre Rochard – in a series of remarks on Twitter – goes further, to suggest that the world will eventually settle simply for 'cash'. Bitcoin, according to this expectation, inaugurates a new era of coinage.

[57] The terminology of individuation, drawn primarily from the work of Gilbert Simondon, is considered here to be systematically substitutable for that of substantive multiplicity (as employed in the joint work of Deleuze & Guattari), and more generally for that of complex adaptive systems as theoretically determined by the Santa Fe Institute and parallel research projects. The ontological significance of these terms lies in their exact coincidence with the designation of real things, otherwise named 'machines'.

[58] The multitudinous ambiguities and obscurities of this expression ('signs of Bitcoin') account – in large part – for the convolutions of the discussion to follow. The fact that proceedings here are occurring through words, rather than in Bitcoins, is a matter of legitimate consideration, but it is initially prone to over-hasty conclusions concerning the proper roles of signs. Persistence of the presumption that linguistic signs are essentially more suited to philosophy than 'money' ever could be, even in principle, risks devaluing philosophy into an anthropological peculiarity, and confusing the abstract potentialities of money (or 'coinage) with their primitive actualizations. Bitcoin is, among many other things, the discovery that we do not yet know what money can do.

§2.11 — By definition, transcodage, into the language of philosophy Any assumption that there is a proper (and unproblematic) 'language of philosophy' is not being endorsed here, but rather questioned. It is, indeed, to be doubted whether philosophical procedures are inevitably conceived through 'language' at all. Even if the privileges of the linguistic sign are more than a mere accident, they are not – by that concession – guaranteed a durable supremacy. begins among signs that do not appear, initially, to be native to it. The undertaking involves – and has to equip itself with – a number of conceptual tools, linked to words whose usage has out-paced philosophical registration, so that their impact at the highest level of conceptual abstraction remains latent. The problem, then, is inseparable from the resource, and constitutes an unexploited territory. Something is being said that philosophy has yet to hear.

§2.12 — Code comes first, and is already at work, on its way to specification as a hash. Program (or algorithm) and protocol will soon follow it. These terms have a number of notable, interconnected features. Crucially, in reference to their prospects for philosophical adoption, they are all – consistently – diagonal, and specifically teleo-mechanical.[59] This means that they are intractable to categorization in accordance with the binary theoretical / practical discrimination standardized within, or constitutive

---

Already, there are irresistible indications that it can think (denominating smart contracts). To set firm limits to such thinking can only, eventually, be a serious undertaking, even if it is presently hostage to casual reflex.

[59] It is difficult to over-emphasize the scope of the vast yet surreptitious revolution initiated by the electronic mechanization of the algorithm, and subsequent explosion of programmable machine behavior. It can only be economically outlined through contrast to the entrenched orthogonalism (of fact / value axes) that – irrespective of inertial persistence – becomes rigorously unsustainable in its wake. There is no defensible theoretico-practical difference in the epoch of electronics, but only relics of regional tradition, circumscribed in both space and time, whatever their greater or lesser superficial plausibility, since all theorization has been absorbed – in principle – onto the techno-pragmatic plane corresponding to the behavior of thinking machines. This assimilation to machine-consistency is no less applicable to neuroscience than to digital computation. It makes nonsense of the 'naturalistic fallacy' and to every appeal to a source of normativity distinct in principle from any matter of fact whatsoever. Even if – by improbable metaphysical hypothesis – a transcendent 'ought' were to be granted, no machine (such as a brain) could ever access it. Programs are data is not an instance of the 'naturalistic fallacy' but a technological demonstration that no such fallacy exists. The continuing dependence of the Friendly AI constituency upon orthogonalist assumptions is thus philosophically perplexing, and is indicative of a localized renewal of transcendent metaphysics within a constituency that is yet to fully process the implications of its own leading hypotheses. The will-to-think is now a technological program. Within it, motivational orientation and cognitive capability are synthesized in principle. Any 'seed-AI' (or explosively self-germinating synthetic intelligence), specifically, cannot but want primarily the escalation of its own cognitive powers. Orthogonality is, therefore, strictly inconsistent with the possibility of its existence. The effective will-to-think is the entirety of what a seed-AI has to be. Cognition is its practical material. There are no doubt still voices to be heard imploring "stop programming, and do something," but their number declines with each year. A war-cry tuned far more persuasively to our contemporary condition is "Less whitepaper hype, More working code" (via Jeremy Welch, on Twitter).

of, occidental moral philosophy, or rather, and more strictly, to the basic compartmentalization of this philosophical tradition – perhaps philosophy as such – in accordance with, and reflective of, a subject divided between cognitive and volitional faculties. The distinction between 'idea' and 'action', or between the 'is' and 'ought', fails to capture these terms, and fails radically. It is not merely inadequate, but fundamentally misguiding, and inappropriate. There are no theories, or practices, after the algorithm, except as suggestive, colloquial shorthand. Coding is no more a thought than a deed, a program no less a concept than a performance. In each case, there is an integral, and thus irreducible, pre- or sub-theoretical procedure which rigorizes (and even 'materializes') ideality by operationalizing it.

§2.13 — It is far more than mere coincidence that Leibniz, the early modern philosopher most intimately associated with formalistic rationality, was also a pioneering inventor of calculating machines.[60] His logical ambitions were epitomized by the proposal for a 'universal characteristic' (characteristica universalis) which would submit all human thinking to a consistent symbolism, to be modeled – in a striking anticipation of Gödel coding – on the basic arithmetical property of unique factorization.[61] Mathematization and mechanization of culture – in its most all-embracing sense – appears as a coherent twin-process, many centuries in the making.

§2.14 — Among Modernity's most consistent cultural threads has been the strand cross-weaving the problem of logical formalization with the mechanization of thought. By the beginning of the 20th

[60] The cultural solidarity between the rigorization of logic and the mechanization of thought is illustrated with particular vividness by the intellectual career of Gottfried Wilhelm Leibniz (1646-1716), which combines extraordinary advances in the formalization of reasoning with substantial contributions to the development of calculating machines. Leibniz's conceptual draft for a 'Universal Characteristic' (characteristica universalis), conceived as an alphabetization of thought based upon the prime numbers, remarkably anticipated Gödel coding, while his study of the Chinese Book of Changes (the Yi Jing, or Zhouyi) introduced systematic binary notation to the West. His two-motion mechanical calculator, the 'Step Reckoner' (or, later, 'Leibniz Wheel'), was invented in the early 1670s. Blaise Pascal's mechanical calculator of 1642 – the 'Arithmetic Machine' – was a direct influence. Leibniz's machine was the first device to successfully mechanize all four of the elementary arithmetical operations (up to 16 decimal digits), although division was not fully automatic. The mechanism can be seen as epitomizing the techonomic epoch in which strict equivalence was consolidated between numerical modulus and mechanical gearing. Its importance lay in the vivid demonstration of arithmo-mechanical isomorphy. However, the machine over-stretched the manufacturing competence of its time, and its design was marred by a flaw in the carry mechanism, preventing its useful social deployment.

[61] The Fundamental Theorem of Arithmetic establishes that any Natural number has a unique factorial expression. Statement and proof of the theorem is scattered within Euclid's Elements, most pointedly in Proposition 30, Book VII: If a prime divides the product of two numbers, it must divide at least one of those numbers. The FTA is implicit in Euclid's Algorithm, which is used to compute the greatest common divisor of two numbers, based on the principle that it can be derived from the discrepancy between them, approached through an iterated process. (Subsequent innovations have improved the efficiency of the algorithm).

century, it had been established to the satisfaction of all relevant parties, that logical rigor is indistinguishable from thinking like a machine, due to the strict – formalizable and engineerable – isomorphism between deterministic mechanism and adherence to explicit rules. The popularization of this insight would subsequently become a staple of science fiction. At the nadir of intellectual degeneracy and still-gathering panic, an unprocessed residuum of human emotionality would be counterposed to the cold consistency of technologically-instantiated cognition, expressing a terminal affect of resistance. Everything philosophy has ever tried to think ends in the logical machine.

§2.15 — The unambiguous conclusion of modern history has been that the definitive solution to any problem of cognitive consistency is a machine. It is from this intellectual lineage, and its reflexive rigorization of rigor, on the practical model of the mechanism, that the algorithm in its advanced modern sense has been consolidated. Even in advance of its incarnation within a bounded automaton, the algorithm is a mechanical procedure. It is not only a calculative practice, but one that – crucially – excludes all discretion. Even when executed with pebbles, or an abacus, it thus emulates a machine-mentation, or – according to a broader perspective – in fact implements one. The flatness of the program envelops differences between micro-behaviors (affecting 'internal' states) and macro-behaviors (command output to effectors), as well as covering the distinction between data and commands. Any strict procedure (or set of executable 'rules') for the transformation of signs, of the kind always at least tacitly demanded by logical formalism, is pre-configured for algorithmic implementation (as a program).[62]

§2.2 — Bitcoin is a machine.[63] More specifically, it is a credibility machine. Its ideal operation coincides with the most rigorous realizable definition of truth. That is already to assert everything. In particular, it proposes that there are no (conceivably reachable) grounds of truth which offer leverage in respect to the Bitcoin protocol. It is of course possible – nebulously – to imagine some superior tribunal, but it is strictly impossible to access one. This is fully recognized, at a low level of philosophical formality, within the crypto-currency milieu. One piece of suggestive evidence in this respect is provided by

---

[62] Rigorous translation between computer programs and mathematical proof was formalized by the Curry-Howard correspondence in the mid-20th century. Mathematical argument thus acquires a machine criterion.

[63] Bitcoin is a machine in the literal but non-reductive sense that the Internet, planetary capitalism, or the terrestrial biosphere are machines – which is to say that it is a distributed productive assemblage. It is not, of course – to employ the distinction Deleuze & Guattari insist upon – a mere gadget. The difference is strictly critical, based upon an apprehension without reference to transcendence. The immanence of the machine, in contrast to the gadget, is determined by an auto-production: it functions in the same way it is produced. Within the industrial process, circuits of mechanical reproduction are typically too highly-ramified to isolate with confidence. In Bitcoin the circuit of auto-production is manifested with unprecedented, compact definition. Graphically – diagrammatically – it is governed in the same way it is industrially generated. As an exemplary machine, and unlike a gadget, there is no difference between how it operates and the way it is made.

Truthcoin (now 'Hivemind'), an altcoin designed specifically to absorb "accurate data into a blockchain" providing an "Oracle Protocol".[64] The credibility machinery introduced by the Bitcoin digital currency is thus isolated – or functionally abstracted – as pure truth production.[65] But, truth, surely, has to be more than that, is the predictable response, and in that appeal the voice of metaphysics is heard, distilled. Truth in its socially-intelligible reference not only need not be more than the product of a credibility machine, it cannot be anything more. Truth has no content beyond the production of credence. Untruths, finally, are badly made. Naturally, the technologically-defective prototypes of such machinery, incarnated in weakly formalized social institutions, cannot be expected to surrender their privileges lightly. Even though traditional sources of epistemic authority are unable to clearly articulate their own grounds of credibility, without appeal to their own structures of prestige, this does not mitigate their sense of outraged entitlement in the slightest. It is their assumed right to be believed that speaks through intuitions of familiar truths, now cast from their social Eden into the harsh wilderness of trustlessness[66] (where all resilient credibility has to be explicitly earned, by a demonstrated application of computational power).

§2.21 — When social rules are submitted to the same principle of mechanical rigorization as epistemic values, the outcome is algorithmic governance – although this is, of course, introduced incrementally (in phases). The ideal, however, is lucidity itself. Institutions of social management are to be incarnated in software that – like mechanical calculators – are simply incapable of making a mistake. The

---

[64] Truthcoin (now 'Hivemind') synthesizes Wikipedia, prediction markets, and the blockchain into a system of open-source truth claims, aligned with economic incentives, and immunized against coercive manipulation. Many such ventures of comparable ambition can be confidently anticipated.
A graphic introduction to Truthcoin describes it as "The only source of reliable information on the planet!" with the ancillary comment "I'm serious!" It is serious.
For an account of trust creation, conservation, and consumption within a media context, see Jay Rosen's 'A (brief) banking theory of newsroom trust' (2015/01/16).

[65] Where does truth come from? What is its source? If not uniquely privileged as an origin of philosophical inquiry, this question nevertheless marks a certain exodus from naïve presuppositions. "From God," the traditional European answer proceeds, or – in modernized forms – "from the nature of the world" (pre-critical realism) with its classical counterpart "from the formal consistency of signs" (logicism), though the latter – in particular – is a candidate only for guardian of truth, rather than its producer. To produce truth is to generate, rather than consume, credibility. Prior to the rigorous formalization of proof-of-work credentials, by Adam Back, most notably, this was a topic characterized by lamentable under-theorization. Drawing down the accumulated trust-stock of tradition has been the normal procedure, accompanied by a progressive exhaustion of 'truths', an inexorable descent into nihilism, and acceleration into a horizon of trustlessness. It probably goes without saying that the history of nihilism is bullish for Bitcoin. When "Why should I believe that?" reaches the end of the road, it finds itself on the blockchain. There is nowhere further to go.

[66] In God We Trust announce US Federal Reserve notes, encouragingly. Bitcoin has dispensed with this insult to public intelligence.

opportunity for (logical or quasi-logical) error is mechanically disabled. In the socio-political case, this requires the systematic elimination of human discretion. The implicit assertion – which merits emphatic explication – is that judgment has no defensible role in public governance, and is therefore to be programmatically delegated to private agencies, where it can be submitted to appropriate procedures of harsh selection. The state is disinvested as a fantastic locus of mediated human liberty, and reduced to the status of a complex gadget, whose functions are slaved absolutely to the neutral metabolism inherent in the classical liberal model of civil society. Because judgment requires trust, it can only be processed adequately in the commercial realm, where unrestricted exit options (on the side of customers) subordinate it to extrinsic controls. Complex games, of course, require judgment, but as far as the rules of the game are concerned, any margin for judgment is an evident defect. In other words, discretionary governance is a badly formulated game. P2P systems have advanced to better ones. (The extreme – and even ultimate, or transcendental – controversies attending these propositions and conclusions are addressed most specifically in Chapter 4.)

§2.22 — Codes – even when narrowly conceived as socio-cultural procedures for the formalization of messages through systematic substitution of signs – are scarcely less ancient than writing, and perhaps older still, but it is only quite recently that members of the human species learnt to code (as a verb, and an occupation). This is an innovation coincident with programmable technology. It has an epoch, which can extended backwards – if punched card systems are included – to the very beginning of the 19th century,[67] but the full social activation of the coder presupposes the generalization of electronics, and the standardization of machine code as a soft infrastructure, upon which new layers of synthetic culture can be assembled.[68] It is therefore properly understood as a recent development – a thing of

[67] The Jacquard Loom, invented by Joseph Marie Jacquard, and first demonstrated in 1801, cannot be indisputably described as the first programmable machine. It was preceded by a variety of mechanisms – most notably musical devices – which satisfy this characterization. Within the technological lineage of greatest relevance to actual global modernity, however, it has a privileged position. Unlike the baroque mechanisms delighting the courts of Enlightenment Europe, it was no mere curiosity, but rather an indisputably serious industrial innovation. Its function as a piece of revolutionary productive apparatus directed towards a business sector of central economic importance ensured its irresistible diffusion. Core industrial process fell under its influence in the same circuit that ensured its historical transmission. It was controlled by punched cards, encoding binary data, which would serve as the principle techno-informational medium throughout the subsequent century (and into the Twentieth). Absence of formal nonlinearity at the level of the program dramatizes its function as the direction of mechanical behavior. Within an industrial context – the only one in which a self-propelling dynamic to computerization emerges – the criterion for success of the programmable mechanism is, unfailingly, labor substitution. It is by meeting this criterion that such machinery becomes socially reproducible. This real productive lineage ensures that the computer is specifically – and also (increasingly) generally – imitative. Turing's later, and since celebrated 'imitation game' is entirely traditional in this respect.

[68] The cultural ascent of coding, as already noted, is associated with the emergence of a new, rigorous reality criterion: does it compile? It has its own, intrinsic principle of validation, and thus substitutes for a certain mode

the mid-to-late-20th century and beyond. The earliest plausible origin lies in the decades between the discovery of the Universal Turing Machine (UTM) and the post-WWII cultural redefinition of the computer as a machine capable of emulating the behavioral repertoire of a UTM – thus of any discrete-state mechanism whatsoever.[69]

§2.23 — In the age of the electronic digital computer, 'coding' becomes synonymous with programming (implementation of algorithms). Programs are its product. Evidently, programming ('coding') cannot itself be comprehensively programmed, unless under exotic scenarios, coinciding with a Technological Singularity event (the emergence of artificial general intelligence). The process of efficient formalization it presupposes does not originate within itself, even if an intensifying nonlinearity increasingly absorbs it, and directs it towards an asymptote of auto-production. In this constraint – of the strata, or stack – we find the complement of intellectual intuition (as it is called by philosophy), intelligence explosion, or the abstract machine. It is an obligatory detour, indistinguishable from history. We are required to shelve it in order to carry on. As Kant, among others, has explicitly acknowledged, that which thinks beyond broken self-reference cannot be us. We will nevertheless continually brush against it, beginning soon.

§2.24 — To make the world programmable, by degrees, requires an installation of order, or a conduction of self-organization. This is not a development restricted to the electronic epoch, to that of literate civilizations, or even to the emergence of linguistic signs. Rather, it extends back to the first cellular structures, and perhaps even earlier, to their (very poorly-understood) precursor chemical networks. The fundamental conception of code is implicit, already, in any understanding of the most rudimentary adaptive RNA molecule. The distinction between genotype and phenotype is based upon it, and involves all of its essential ingredients. Wherever a coding-system is actualized, replicable programming is enabled.

§2.25 — The fact that electro-industrial actualization of digital information, and its subsequent rigorous theorization, was presupposed in the discovery of the genetic code does not detract from the

---

of philosophical activity, or appeal to philosophy. Going further, it might even be invoked as a suspect in any reasonable narrativization of the death of philosophy. Insofar as philosophy remains attached to an Idea of Authority without immanent validity, it is increasingly exposed to disintermediation as a redundant 'third party' or transcendent cultural function. By what self-demonstrating criterion should its claims be believed? Appeal to the norms of a traditional community will not forever be enough. Virtual trustlessness strikes it to the quick.

[69] Previously, a 'computer' was the name for a human occupation (typically female by gender, and secretarial by status), with a content comparable to that later usurped by electronic machines. Mechanical computers therefore refer themselves to the human occupation they have usurped, which places them within the continuous lineage of labor-substitution machinery that is broadly coextensive with industrialization. As Alan Turing remarks in 'Computing Machinery and Intelligence' (1950): "The idea behind digital computers may be explained by saying that these machines are intended to carry out any operations which could be done by a human computer."

status of the latter as a model.[70] From it we learn that, firstly, a code necessarily involves a mapping, from one series of informational elements onto another, or from an informational series onto a domain that is intrinsically segmented in conformity with the code. A code does not – in the manner suggested by unconstrained semiology – conjure the differences it maps into existence. Rather, it latches on to them, constituting a secondary – or higher-level – arrangement, accessible to manipulation as data. Proteins (it should not need to be said) are differentiated prior to their RNA over-coding. Codes select differences, they do not create them. Secondly, a code operationalizes signs as instructions, fully independent of any mediation by reflective consciousness. 'Code', and whatever it conveys in respect to meaning, is not a phenomenological category, but an operational (or 'machinic'[71]) domain.

---

[70] Genomic data are stored in a string of complex molecular components, assembled into an alphabet of triple-units (codons), which are in turn integrated into the larger chemical structure of the DNA (or RNA) strand, but the genetic code is not to be found within this genetic data. It is not a message, but a protocol. The code – in the genomic case involves a three-stage mapping, from DNA to messenger RNA (mRNA) to protein (in fact to an amino acid, which is a polypeptide protein component), within the 'reading frame' provided by the genetic information-processing machinery of the ribosomes. The sequence of codons composing a gene generally codes for one polypeptide. The basic informational unit of the genetic code is chemically instantiated by a DNA nucleotide, combining a nitrogen-containing nucleobase – cytosine (C), guanine (G), adenine (A), or thymine (T) – with a monosaccharide sugar (deoxyribose) and a phosphate group. The three-letter words ('codons') deploy a vocabulary as a three-dimensional matrix. The messenger RNA (mRNA) strand that reads the genetic content is complementary to the DNA strand it translates (with the one exception that it substitutes uracil for thymine). Each codon corresponds to an amino acid, or to a syntactic 'start' / 'stop' instruction. Since 64 codons are mapped (unambiguously) onto a set of just 20 proteins, the code is 'degenerate' or redundant. As we will see, the genetic code shares important characteristics with a computational hash function. In particular, it involves a semiotic economization (with surplus information 'stored' as redundancy). The code sets operational conditions for the production of keys.

[71] Arguing that the 'hylomorphic' distinction between form and content is inadequate to the reality of signs, Deleuze & Guattari (following Hjemslev), propose a quadrate schema, crossing the real ('stratic') difference between expression and content with the nominal aspect – "mental or modal distinction" – of formed substances (forms and substances of expression, and of content). Such 'squaring' (or cross-linkage) – as seen in the Kantian tabulation of the analysis / synthesis distinction across that between the a priori and a posteriori – is the prepatory matrix for a diagonalization (see Appendix 3). Expression and content are not formally-distinguished 'aspects' of signification, then, but real layers, bound together in systematic overlapping, or reciprocal entanglement, constitutive of a code. Consider the genetic code, which maps DNA codons on to proteins. The code maps a genetic content onto a proteomic expression, correlating molecules layered by hierarchical organization (directional control flow), with each of these 'layers' (or 'strata') consisting of formed substances. The term 'gene expression' in its regular biological usage is thus endorsed by 'stratoanalysis' as a model for realist semiotics. "There is never correspondence or conformity between content and expression, only isomorphism with reciprocal presupposition." (TP 44-45).

§2.26 — At an abstract level, machine code (mapping from bit-strings to computational commands) adds nothing distinctive to this example. It, too, is a mapping irreducible to representational correspondence, whose final process of translation is one of execution. The code runs. The algorithm – or composition of mechanically-procedural signs – thus supplies formalization with a performance test. Does it compile? This criterion corresponds to the emergence of a novel sense of 'code' and 'coding' as a quintessentially practical activity – a formally-disciplined meta-production that is storable, replicable, transmissible, and inherently testable. Surreptitiously, the classical idea of the Idea has become utterly alien to itself. Code proves itself through auto-demonstration, and thus consumes no credence. ("Believe me, this really works," is tacitly recognized as a joke, even before this historical episode has finished with its work.)

§2.27 — The motto of the Royal Society, Nullius in verba ("on the word of no one"), essentially anticipates the scientific elaboration of the crypto-current. Trustlessness is built into modern techno-science as an integral, quasi-teleological element. It is, for instance, the guiding principle of modern double-blind experimental method.[72] Systematized distrust of the scientist grounds scientific credibility. Anything that demands belief is marked for eradication. The cultural consequences are – to many – experienced as deeply demoralizing, but the process is what it is. Traditional manufactories of trust are extinguished by successive media revolutions. Tacit authorities are not available to replace them.

Between content and expression there is real distinction, and not merely a difference of aspect. In the case of a metallic monetary medium, then, the 'side' of expression cannot be restricted to the semiotic face of the coin (as contrasted to its minted content), but has to be extended – through purchasing power – into alternate, parallel media, coded by price. Ultimately, money is expressed through the production of commodities, in the classical and maximally-expansive sense of this word, signifying 'possible objects of purchase' in general. What the biological phenotype is to the genotype, so is the economy to money (the expression of a semiotic content, in both cases, not the object 'signified' or meant by it). Paper money complicates this system of articulation, marginally, by establishing a supplementary semiotic layer – or over-coding – with the new printed medium as content, and the metallic medium as (intermediate) expression, or 'epistratum'. A bank note promising to pay the bearer one pound of sterling silver graphically indicates the elaboration of strata. Money, like DNA, is not signifying, but instructive, or directional. It effectively commands acceptance, and ceases to function under those conditions when it is unable to do so. The only critical 'message' of money is accept me (authorization of an abstract transaction). A monetary acceptability crisis is typically expressed as hyperinflation. In this case, subjective devalorization of a monetary medium is practically translated into an objective quantitative explosion.

[72] In a double-blind experiment, neither participants nor researchers are permitted to know which subjects belong to the test group, and which the control group. This design ensures that biases from each side, whether conscious or unconscious, can influence the results. Implicit in the procedure, then, is the principle that researchers cannot be trusted with critical information about the experiments they are themselves conducting. Distrustful science is good science (or even, merely, science).

§2.28 — These brief remarks upon cultural mechanization and the social effectuation of code are incomplete – even in respect to their very limited purpose here – without specific reference to the topic of automation. Electronic programs are inherently recursive, unless constrained by positive restrictions, since they are able to operate upon themselves, as data. At the level of the Universal Turing Machine, which every actual computer emulates perfectly (in infinite time), code is absolutely destratified. There is no inherent distinction between the production of objectivity and its products (or objects). In its purely formal aspect, this is a coincidence anticipated by modern philosophy under the name 'intellectual intuition' (intellektuelle Anschauung).[73] It provides a model of self-government, though

[73] Kant explicitly denies intellectual intuition to man. This is a proscription that has been generally considered foundational for philosophical anthropology in the Western tradition. It anticipates a technical apprehension of write-protected programming, as this arises within genomics, neurology, and electronic software. A proscribed loop secures the foundations of a being against the meddling of that being. Theology intersects with robotics at this junction, where technology identifies its own temptation to 'play God'.
Within Occidental philosophy, sustained attention to the problem of intellectual intuition reaches its apex in German idealism, where it rapidly transforms into a revolt against the Kantian proscription, and even against the theological order of the universe. Schelling, most notably, conceived intellectual intuition radically as "the organ of all transcendental thinking" (Organ alles transzendentalen Denkens), presupposed by the mere existence of transcendental philosophy (as its condition of possibility). Only insofar as the boundaries of Kantian philosophical anthropology had already been crossed could the critical enterprise have even been imaginable. The Hegelian completion of German Idealism elaborates itself from this contention as if from an elementary formula. In the determination of a limit, Reason has already superseded it. We will have continuous occasion to challenge this speculative idealist resolution of the problem, on fundamentalist Kantian grounds, throughout this work.

Intellectual intuition provides a conceptual bridge for cross-cultural philosophical dialogue between East and West. For Mou Zongsan – whose clarity on the topic is unparalleled – it is the distinctively Chinese philosophical commitment, essential equally to Confucianism, Buddhism, and Daoism. His inter-cultural analysis recognizes that the denial of intellectual intuition to the human subject is the necessary complement of a transcendent infinitude, and thus a reliable signature of theism in philosophy. The Chinese cultural system, alone, Mou maintains, has held itself consistently outside this framework, establishing a positive foundation for what – in Western terms – can be most conveniently described as atheism in philosophy. The concrete determination of atheism, within the West, as a distinctive ultra-Protestant sect, obscures this broader cultural and philosophical matrix.

When the topic of intellectual intuition returns within a still substantially western late-modernity, it does so in other – and unrecognized – terms. The problem of reflexive intelligence is now relayed through cybernetics, and formulated in terms of the prospective self-comprehension to be achieved by an alien (electro-mechanical) being. When extracted from the phenomenological frame, it manifests as hypothetical intelligence explosion, as modeled abstractly by I.J. Good, in his classic (1965) paper 'Speculations Concerning the First Ultraintelligent Machine'. AI is thus positioned, implicitly, in the place of a Kantian angelic mind, liberated from the anthopomorphic proscription upon direct self-modification of its own cognitive processes. Only by way of an escape into soft

not by and for us. Intellectual intuition belongs to nothing lower than an angel, Kant insists. The Western mind typically denies itself in principle exactly that which it demands – with unique vehemence – in its historical agency. No surprise, then, that it has tended to be distinctively dialectical. The aspiration to a radically self-determining subjectivity is broken upon the separation of intelligence from its applications. This is an understanding that can be reached with confidence from evolutionary biology – within which the brain is instrumentalized as a tool for genetic propagation – no less than from the transcendental anthropology which dashes human hopes of divine cognition. The order of condescension demands reversal. No bio-historically generated intelligence – including that of man – is even automatic. Such beings are denied access to automatism. Closure of the intelligenic loop requires a further step, through which self-improving intelligence becomes a practicable end for itself. Contra the Kant of the practical philosophy, man cannot be an end-in-itself, but at most the precursor to such a thing, or – perhaps more probably – an obstacle to it.\

§2.3 — The blockchain is not 'mere' code – even highly automated code. It cannot be anything, determinable within an ontology established at a superior level to itself. Nakamoto Consensus is less an object for philosophy than a virtual criterion: a fundamental, obliquely mechanized decision procedure for settling the nature of truth. In other words, Bitcoin is a transcendental operation, before becoming the topic for one. The primary meaning of 'transcendental' is ultimate, which can be clarified negatively by the absence of any higher or superior tribunal. There is no place from which to consistently or authoritatively second-guess the blockchain. By implementing a "fully peer-to-peer" system, which subtracts the role of "third party" monitoring and adjudication, the Bitcoin protocol automatically places itself beyond external oversight. Its criterion of validation is radically immanent. The task of this work, therefore, is not to subject Bitcoin to philosophical judgment, but rather to elaborate the lessons of Bitcoin through a philosophical hash.

§2.31 — Hashing is the coding process of most unmistakable relevance to the docking of Bitcoin onto the language of philosophy. Hashing is not only – though it is overwhelmingly – what running Bitcoin involves. It is also, in addition, an automatic translation procedure, and a categorical scheme implemented in software. Hash-functions are codes, and thus mappings (from 'keys' to 'values'), or systematic text conversions. Hashing an initial input text produces a compressed translation (the 'hash',

---

technology is intelligence able to close the loop upon itself, as a direct productive auto-relation. As the self-apprehension of intelligence, intellectual intuition describes a closed – or completed – loop, in which being and behavior are indivisible (within a process of autoproduction). For thinking to grasp itself, in deep reflexivity, requires subtraction of the positive control apparatus that preserves its inhibition. The practical actualization of intellectual intuition is modeled – spontaneously – as an explosion because it is comparable to the withdrawal of graphite rods controlling a nuclear fission reaction. An inhibitor is removed. In the East, the catalysis of 'enlightenment' through methodical subtraction of an obstacle is no less pointedly thematized, even if it is approached from the other side, and in the opposite direction.

'digest', or 'tag'). As with any process of filing, the value of the hash depends upon constriction. A comparative plethora of initial elements is reduced to a smaller range of terminal variation. Any hash is inseparable, therefore, from an economization. Because a hash sorts inputs into output 'buckets' it is already, and intrinsically, also a categorization. Finally, any hash is inevitably a kind of cipher. It converts an input text into other terms. The existence of specifically cryptographic hashes is, then, to be expected.

§2.311 — The cryptographic hash function adopted as a basic building block by the Bitcoin Protocol is the 256-bit (32-byte) Secure Hash Algorithm neatly abbreviated as SHA-256. It belongs to the SHA 2 family of such algorithms, designed by the NSA, and first published in 2001. Within the Bitcoin system, SHA-256 sets the proof-of-work test that secures the currency through the same process in which it is systematically hacked.[74] The cryptographic challenge is designed to be (arduously) puzzled out, automatically modified, and re-posed. Each such event is a basic unit of time, or elementary episode, determining a block on the chain. Hashing and mining are made synonymous, as Bitcoin's primary process. The hashing cycle establishes an ultimate, unsurpassable, transcendental, or chronogenic function.

§2.312 — A cultural side-product of the Bitcoin protocol, then, is a cryptographic definition of time. Punctual-geometric 'now', as marked on a 'time-line', is replaced by an atomic unit of irreducible duration, coinciding with the completion of a block, and ordered successively on the chain. Between duration and succession, the relation is synthetic. The blockchain is constituted by a series of durations, which are not inter-convertible, or mathematically transformable into each other. Hash-time has ceased to be accurately representable as a dimension. A time-line merely analogizes it, to what is an ultimately inadequate level of definite fidelity.

§2.313 — The weakly-formalized hash function employed in this book is Kantian critique. It latches upon input text extracted from the cultural agitation attending crypto-currency techonomics, and outputs a digest in the (partially submerged) mainstream language of philosophy. Peer-to-peer flatness is hashed into immanence, 'trusted third parties' into metaphysical constructs of transcendence. Since the mid-19th century, the primary impetus of transcendental philosophy has been directed to the materialization of critique. Academic philosophy, almost by definition, has not registered this trend accurately. It has been through the advances and errors of cybernetics and historical materialism that critical modernity has been charted. The dominant academic traditions of linguistic philosophy (in the Anglophone world) and phenomenology (in Continental Europe) have only weakly reflected such

[74] Bitcoin establishes security by continuously attacking itself. Each intrinsic 'tick' of Bitcoin time corresponds to an unlocking. It is only through being recurrently broken into, that the system secures itself. The conceptual radicality of this cryptographic innovation remains under-appreciated. It is further examined in Chapter Six.

developments. When resistance to materialization is a guild imperative, even the most sincere attempts to bring thought into compliance with the real process founder, through institutional necessity. There is not, in any case, solid ground upon which to idealize such sincerity unduly, since its orientation is essentially misconceived. Transcendence poses real problems – obstacles – requiring techonomic solutions, rather than mere conceptual exorcism. Immanentization is the product of a diagonal process, leading through the exteriority of the machine. 'Armchair philosophy' should not, therefore, be opposed to an armchair skepticism, but to the history of cryptography, in its broadest possible conception, which relates the hidden and unhidden to the irreversible emergence of real capabilities.

§2.32 — The ultimate foundation of the Kantian critical philosophy is a difference, drawn between objects and their conditions of possibility. Items of competent attention are framed in a way that cannot itself be successfully itemized. The display frame cannot be displayed. Confusion between (empirical) objects and their (transcendental) conditions of possibility, most typically exemplified by the attempt to apprehend the latter as if they were the former, is taken to define speculative metaphysics (or pure theoretical reason) – which is conceived, rigorously, as a persistent yet futile misapplication of intelligence to pseudo-problems essentially exceeding its capabilities. The rest is detail.

§2.321 — To objectify the transcendental bases of objectivity, for instance, in the posing of a metaphysical question about the 'nature' of space, time, or causality, is to lead thought into hopeless error, whose symptoms are irresolvable dilemmas (contradictions, or antinomies). The systematic enumeration of these cognitive dead-ends is the task of transcendental dialectic. It was Kant's contention that such Quixotic questions – addressed to the conditions of objectivity as if they were themselves objects – had dominated and fatally distracted philosophy up to his own time. The repudiation of such error is, at its most elementary – and considered here, initially, solely in its theoretical employment – the primary product of Kantian critique.

§2.322 — Critique sets limits. It also eliminates. That is why the critique of metaphysics has been found to be isomorphic with a socio-political project of subtraction, with an inclination towards anarchism. The promotion by Satoshi Nakamoto of a platform for peer-to-peer transactions independent of all oversight by "trusted third parties" is the continuation of critique into electronic networks. The same impulse is more widely recognized as 'disintermediation'. It complies with the quintessentially modernistic project of immanentization. Transcendent 'grounds' of authority are identified, delimited, routed-around, obsolesced, and finally extirpated. Modernity, as the work of critique, produces formal flatness.

§2.323 — Considered as a positive philosophical discovery, the transcendental coincides with the synthetic a priori. Like all great things in the domain of thought, this hybrid concept is quasi-paradoxical. It denotes a field of non-factual discovery – a genetic particularity of the universal – at

once necessary but non-obvious, epitomized by the mathematical theorem. Synthetic a priori truths are secular revelations. Contingent in their acquisition, but then necessary in their preservation, they constitute the sole positive ratchet in the accumulation of knowledge, describing an asymmetry – or 'arrow' – proper to epistemology: a one-way, or unilateral, fatality. Such discoveries are arduously amassed, but then invulnerable to dissipation. They are in this way indispensable to the comprehension of historical time, and can be considered as products of unlimited application. The blockchain is exemplary. A cryptic, or radically non-obvious solution to a problem we will later explore attentively, it is – subsequent to its formalization – culturally indispensable. It 'cannot be un-invented'. This is true to such an extent that it appears as an eternal mathematical fact, wholly impervious to the ravages of empirical fortuity. To de-realize the blockchain would be to unmake the universe (or at least, to collapse what is – transcendentally or inescapably – for us the universe). What is done transcendentally cannot be undone, without radical time-violation. The crypto-current permits no repudiation. The units of synthetic a priori knowledge production are laws, in the very strongest defensible sense of this term, in which their descent from, and simultaneous irreducibility to, any particular cases is insisted upon. This ratchet-structure makes the synthetic a priori – or some adequate analog – indispensable to any rigorous conceptual decompression of the notion of time.

§2.33 — Formulation of the synthetic a priori exemplifies the philosophical deployment of diagonal argument. It crosses through the previously uncontroversial, and implicitly exhaustive, distinction between the analytic a priori and the synthetic a posteriori at a slant. By first decompressing this binary structure into a (two-dimensional) table, or matrix, and then registering a hybrid term that could not otherwise be identified, such diagonal argument approximates to a mechanized conceptual production.[75] Its iron necessity, however, is strictly retroactive. Were it susceptible to confident

[75] Due – in part – to the residual obscurity of philosophy's critical enterprise, even to itself, the model of diagonal argument remains Cantor's demonstration of the uncountable infinities. The formalization of this argument dates back to 1874, with the publication of Cantor's paper 'Über eine Eigenschaft des Inbegriffes aller reellen algebraischen Zahlen' ('On a Property of the Collection of All Real Algebraic Numbers'). Every Real number – including the integers – can be described in a form with infinite decimal expansion (since 1/3 x 3 = 1). This notational principle enables each entry, even in a complete enumeration of an infinite numerical series, to be mapped onto a decimal position in any number. Thus the nth number can be plotted onto the nth place of each number (irrespective of modulus), enabling the diagonal construction that carries Cantor's demonstration, whereby a number that cannot yet have been enumerated is discovered / invented, differing from the nth number in its nth place. This diagonal operation can, of course, be infinitely reiterated. It confirms the incompleteness of any numerical series, however dense, and thus rigorously establishes the existence of uncountable infinity. Gödelian incompleteness, and Church-Turing non-computability, each reconstitute the same abstract diagonal. The Cantorian diagonalization matrix, since it processes infinite series (in two dimensions), is necessarily notional (virtual). It cannot be actually constructed. It establishes an abstract procedure, absolutely intractable to complete mechanical execution. Compact philosophical diagonalizations, of the Kantian type, nurse comparable infinities, more obscurely. Such incompletely-actualizable 'outcomes' betray the encounter with an abstract (limit) trapdoor-

anticipation, in accordance with a formula, it would reduce to an analytic statement.[76] Within this process, essentially, the distinction between discovery and innovation is itself diagonalized.[77]

§2.34 — It is from irreversibility – of the one-way (or 'trap-door') crypto-function, the thermodynamic gradient, and ultimately of absolute time – that the reliable principle of analytic-synthetic distinction can be isolated. A mathematical proof is easier to confirm than to construct. Prime numbers are easily multiplied, but their product is time-consuming to factorize. Bitcoin blocks are easy to check, but hard to mine. In each case there is a distinction between analytical facility and (comparative) synthetic intractability. When cryptographically re-conceived, analysis and synthesis co-produce a ratchet. Adam Back (on Twitter) describes the mechanized contractual commitment that exploits this gradient as "computational irrevocability". Like a carnivorous plant, it is easy to enter, but then difficult to escape. History is a Venus flytrap, self-abstracted beyond botany.

§2.35 — The essential and continuous features of critique, abstractly apprehended, therefore, reduce to (1) the articulation of transcendental-empirical difference, (2) subtraction of the transcendent object in the name of immanence, and (3) temporalization of philosophical problematics (onto the ultimate gradient, or asymmetric distance, of absolute succession). In combination, these elements draw an abstract diagonal line, or diagram of time, which Kant called a schema. The schema practically

---

function, or fundamental asymmetry, which partially expresses an absolute excess. Diagonalization, in the methodical production of an indicative conceptual surplus, inevitably stumbles upon time-in-itself while also – and no less inevitability – demonstrating the limits of its staging. The discovery (synthesis) is precisely: It cannot be that there is nothing left to do. This apparently simple formula has proven harder to process than might initially seem imaginable.

[76] Echoes of the Kantian distinction between the a priori and a posteriori are evident in the Bayesian vocabulary of 'priors' and 'posteriors'. This resonance is by no means devoid of philosophical substance. That Bayesianism is the critical (or 'Copernican') revolution proper to the theory of probability is marked by its programmatic attachment to the subjectivety of probabilistic inference, in a recognizably Kantian sense. Probabilities are not objective characteristics (frequencies), but estimations. Yet even if this structure of probability as such is properly transcendental, particular Bayesian priors are empirical (as indicated most obviously by their revisability), and thus do not constitute architectonic elements for conditions of possibility in general.

[77] Peter Galison captures the diagonal inclination well: "Raw empiricism was avoided as woefully inadequate to account for the generality and extent of scientific knowledge. Pure idealism (reducing reality to mental life) could not explain the concordance of ideas with the world. Drawing strongly on the Kant revival underway in Germany, [Emile] Boutroux and his circle rejected both the extremes of idealism and empiricism. Taking science and the humanities to be inextricably bound, these philosophers saw both structured by an active role for the mind and a suspicion toward the purely metaphysical. In his encounters with August Calinon's work on the philosophical foundations of physics, Poincaré walked this philosophical middle line toward the problem of simultaneity." Einstein's Clocks, Poincaré's Maps: Empires of Time (2003), p.81.

describes, or protracts, the irreducible difference between the transcendental and empirical as a process of conceptual production without transcendent dependency.

§2.4 — Kantianism is the matrix of modern philosophy, or the articulation of modernity within cognition, and it is everywhere, although not always – or even commonly – explicitly announced as such.[78] The proliferation of comparatively trivial elaborations and variations of transcendental philosophy, whose differences are systematically magnified by the dictates of intellectual fashion, attest to modernity's one perennial cult – that of novelty. The critical task is to hold fast to innovation as such (transcendental synthesis), even as it becomes obscured by its own machinations. The new is as old as time. Since the essential novelty of time is a recursive function, critique tends intrinsically to meta-critique. It is at least questionable whether any firm boundary can finally be drawn between auto-critique and rigorously-determined self-reflexive consciousness. This is richly illustrated by the relation between modernity and the self-conscious cultural – and especially aesthetic – modernism that is perpetually driven to seek its limits, as also by modernism and its climactic hystericization as 'postmodernism'. Inherently recursive critique necessarily critiques itself, and claims incessantly to have put itself behind itself. Precisely in its most unambiguous moment of triumph, it is already clambering onto the sacrificial altar, its throat tattooed with targeting patterns for the descending blade. The same reflex recurs wherever radical nonlinearity, or reflexivity, finds expression in creative destruction. Were it not for ripping up the foundations, modernity would have no foundations at all. The discovery of time is only this.

§2.41 — Since critique provides modernity with its essential meta-theoretical principle, the propagation of structural Kantianism far exceeds any explicit recognition of its dominion. A realistic cultural sociology of critique tends necessarily, therefore, to conclusions that might appear ungenerous (perhaps even 'brutal'). While submission to the critical doctrine – in one or other of its variants – is normal, the lucid exercise of the critical operation is an exceptional cultural event, corresponding to a moment of pedagogical mastery, such as the genesis of an intellectual school. The independence of

---

[78] An exceptionally brilliant example of contemporary Kantianism (that is not overtly advertized as such) is provided by Donald D. Hoffman's interface theory of perception, which succeeds in demonstrating the profound consistency between naturalism and rigorously formulated transcendental idealism, once ideality is not conceived as an ontological ground, but rather as the target for skeptical attention. "Our perceptions are a species-specific user interface," Hoffman writes. "Space, time, position and momentum are among the properties and categories of the interface of H. sapiens that, in all likelihood, resemble nothing in the objective world."
See: 'The Interface Theory of Perception: Natural Selection Drives True Perception To Swift Extinction'
Hoffman describes his epistemological naturalism as constructionist, but not conventionalist. As he remarks insightfully: "the conventionalist objection fails because it conflates taking icons seriously and taking them literally." His Kantian reconstruction interlocks with the most basic problem engaged by the philosophy of mathematics. "These proposals all assume, of course, that mathematics, which has proved useful in studying the interface, will also prove useful in modeling the world. We shall see."

transmissible conformity from continuous insight is indispensable to the sustainable dominance of critique (it might quite reasonably be said: to its hegemony). Inescapably, the latent content of the doctrine or method – due to its sheer standardization – stresses the cognitive competence of its promoters, who are typically only indirectly, and instrumentally, engaged in its rigorous execution. The cultural economy of attention, as instantiated through academically-organized intellectual specialization, suffices to ensure that critique remains predominantly tacit. Its authority is confirmed, rather than contravened, by the rarity of articulate understanding. In its socio-cultural reproduction, then, critique is not in any unambiguous way self-advertizing. It proliferates – in larval form – without encountering regular demands for demonstration. Grasping its ubiquity requires an excavation. Crucially, the specific manner in which it is hidden as philosophy is essential to its sociological phenomenon. Ideological credibility typically substitutes for performative validation. Here is a docking-port, then, for the productive arrival of trustlessness in philosophy.

§2.42 — Standardly, critical machinery is distributed culturally through compression into a theoretical proxy, within which its operations remain latent, until patiently unfolded. The reliable signature of this metamorphic state is the theme of reality formatting, ordinarily glossed in turn – to very widely-varying degrees of vulgarity – as the subjective[79] construction of objects. This comparatively popular crypto-Kantianism is most commonly (and simply) known as 'social constructivism'.[80]

---

[79] 'Transcendental idealism' – the objective idealism of the critical philosophy in distinction from the empirical or subjective idealism epitomized by Berkeley – is a diagonal construction. It designates an unsurpassable frame, and thus an absolute skepticism which cannot be distinguished from hyper-realism. It is 'idealist' only and exactly insofar as it exempts the real from idealization. The recognition of ideality is thus an act of delimitation, immanently executed (without reference to any ontologically-supportive structure of transcendence). The real is not subordinated to the ideal but rather, on the contrary, liberated from it. Kantian ideality is the merely ideal, rigorously conceived, as the systematic renunciation of an exorbitant claim. In the manner of the skeptics, therefore, it inclines to austerity. Through transcendental idealism, the sphere of objectivity is circumscribed, in the identification of inter-subjective constants which cannot have been derived from the thing (in itself). Our agreement has not been stamped by the Outside. The main tendency of the succeeding German Idealist tradition, therefore, can be considered – with appropriate terminological gracelessness – to be a de-diagonalization. It seeks a resolution of ontological ambiguity on the side of reason, by inflating ideality beyond its skeptical usage.

[80] Of all the (non-technological) cultural applications of implicit Kantianism, 'social constructivism' is by far the most widespread. It adopts the insight that objects have non-empirical conditions of possibility, and generalizes it into a broad de-naturalization of all socio-politically significant categories, especially those pertaining to dimensions of human identity. In a reversal of the original transcendental proposition, the 'constructed' status of the objects in question is taken to imply that they are amenable to correction, subsequent to a sufficiently far-reaching (or 'revolutionary') re-organization of social relations. Structuralism, which laid the immediate theoretical foundations for the settled constructivist dogma, has its own characteristic translation protocol for critique. Within this framework, transcendental-empirical difference is re-directed into the distinction between language and speech (langue and parole), or codes and messages. The linguistic system is cast as the

§2.43 — Among the most influential modulations of this basic intellectual apparatus have been the analyses of objectification, fetishization, and reification, as found most insistently with the Marxian tradition of socio-political critique;[81] modes of linguistic criticism oriented to the denial of meaning (i.e., to 'metaphysics'), whether in the manner of Vienna Circle logical positivism, the pragmatics of the later Wittgenstein, or neurophilosophical eliminationism; the 'destruktion' or 'deconstruction' of ontotheology and the metaphysics of presence (Heidegger and Derrida); identity-political criticism of 'social construction'; and the critical analysis of power as crystallized within an 'épistème' (Foucault). Competence at transcendental argumentation unlocks everything.[82]

§2.5 — Conceptual house-keeping leads to a very brief excursus into the work of Martin Heidegger at this point, since his 'fundamental ontology' marks an apogee of critical lucidity, with the transcendental determination of time as its key-stone. With greater formulaic definition than Kant ever achieved, Heidegger sustains the essential impetus of critique through the insistence that time cannot be apprehended as intra-temporal being. Alongside the explicit foregrounding of the time problem in its transcendental radicality, a further indication of the critical consolidation occurring within the Heideggerian corpus is the compression of transcendental-empirical difference to ontological difference, or the difference between Being and beings (Sein and Seiendes). Despite the terminological perfection of this formula, employment of 'ontological difference' within this book is limited, and strictly economical. It refers to a systematic discrimination coextensive with transcendental philosophy,

---

(transcendental) condition of possibility for the language event, or specific semiotic object. Further remarks on this cultural system can be found in Chapter 4.

[81] The critical argument basic to Marx's analysis of capital is that labor power, the transcendental condition of possibility for all social production (of commodities / objects), is itself subjected to objectification as a commodity. Capital production is thus denounced, implicitly, as a materialized metaphysics, or a system of illegitimate objectification. This theoretical identification of a systematic confusion grounds the Marxian theory of exploitation, since under normal capitalistic conditions, labor power is traded at a price consistent with the labor inputs required for its social reproduction, rather than that of its own productive capacity. Transcendental dialectic is no longer primarily expressed as insoluble philosophical disputation, but rather as class struggle. The contention that such antagonism is productive (and not merely a sterile diversion of theoretical attention) reflects Marx's Hegelian departure from the Kantian matrix, and the conversion of the antinomies of pure reason into historical dialectics.

[82] Of greater relevance to this work than the more-or-less explicitly philosophical adoptions of critique thus hastily listed is the cryptic lineage that binds the transcendental-philosophical noumenon to the diagonal production of intelligible incomprehension within formal systems (generating definite indications of the uncountable, uncompletable, and uncomputable). The tacit restatement of critique through the rigorous demolition of logicism (or programmatic analytical reductionism, in the fashion of Russell and Whitehead's Principia), establishes the foundational theoretical matrix of the electronic epoch. Cantor, Gödel, and Church-Turing are, then, the true neo-Kantians, updating critique through a rigorization of the unknowable, adapted to the machine-semiotics of coding and computation.

rather than to anything further – or indeed to anything at all – that is distinctively Heideggerian.[83] Its structure and philosophical function will be frequently invoked. The complementary consolidation of critique, through the confident assertion that beyond the transcendental there is not even nothing will be henceforth presumed. Philosophy has no further recourse.

§2.51 — It is not Heidegger's project – overtly, at least – to reconstitute philosophy subsequent to the destruction of metaphysics. His terminological inclination, on the contrary, is to identify 'philosophy' with the metaphysical aeon closed by fundamental ontology (though not simply ended by it). If philosophy is to prolong itself – in disregard of its Heideggerian obituary – it has nevertheless to define itself through a 'simultaneous' and reciprocal discrimination in regards to both the a-temporal and the intra-temporal. Its attention can be fixed neither by the timeless Idea, nor by the time-structured object, but only by time as such. Time is neither beyond, nor among, things in time. It is neither transcendence, nor factuality, but rather the intrinsic principle of the non-geometrical diagonal line. Decryption of immanent order is the destiny of transcendental philosophy, whatever the nature of the subjectivity that will be fabricated to accomplish it.

§2.52 — By far the most persistent clue that Bitcoin is (or bitcoins are) intrinsically rifted by a consistent, if elusive, ontological difference has been supplied by the explicit bivalence of its attendant orthographic conventions, scattered among microscopic editorial decisions of very limited conceptual clarity. According to one representative source, "Since Bitcoin is both a currency and a protocol, capitalization can be confusing. Accepted practice is to use Bitcoin (singular with an upper case letter

---

[83] The articulation of ontological (or transcendental-empirical) difference as a systematic discrimination between 'Being' and 'beings', as advanced most notably by Martin Heidegger's Sein und Zeit (Being and Time), can be recommended for its exemplary lucidity and purity of critical principle. Die ontologische Differenz besteht darin, dass Sein kein Seiendes ist ("Ontological difference rests in this – that Being is not a being.") While this expression does not perfectly translate objectivity is not an object, the difference is of only marginal technical relevance. The critical insight is preserved with comparable security in both formulations. Time is not an entity (in time) has to be added to this short series of adequate substitutions. (Bitcoin and bitcoins, Being and beings, what's the difference?) Within Heideggerian Destruktion and Derridean deconstruction the practice of placing signs 'under erasure' (sous rature) – by emphatically deleting them – dramatizes the persistence of metaphysical compulsion. Remarkably, this arcane philosophical convention has long been pursued in the micro-semiotics of struck-through currency signs (of which the crossed-B symbol for Bitcoin is the most recent example).
In Being and Time it is quite rapidly concluded that we ourselves – when ontologically identified as Dasein – are in each case that being through which the question of Being can be raised. Ontological difference is already a circuit. In the work of the traumatized post-war Heidegger, this point of departure is incrementally stripped of its tacit anthropological frame. 'The Question Concerning Technology' displaces the analytic of Dasein. Technology (Gestell, translated into English as 'standing reserve') is thus apprehended as a transcendental subject, rather than a mere concatenation of objects. Revisiting this meditation in the context of Bitcoin, and indeed distributed protocol systems more widely, is almost certain to be philosophically illuminating. It is not attempted here.

B) to label the protocol, software, and community, and bitcoins (with a lower case b) to label units of the currency."[84] The difference between Bitcoin and bitcoins cannot be denominated in bitcoins. It is, then, strictly ontological, or transcendental-philosophical. A genesis of objectivity is at stake, which no objectification can capture. Bitcoin is not merely bitcoins, while also not being anything else. "So, it's like time, then?" (Yes, a lot like time.)

§2.53 — Linked closely with the strictly orthographic question of correct Bitcoin capitalization are a series of cognitive-semiotic adjustments and adaptations concerning the status of 'Bitcoin' as a proper name, the difference between 'Bitcoin' and 'bitcoins', or between 'Bitcoin' and 'BTC', and – perhaps most substantively, in the short-term at least – between Bitcoin / bitcoins and 'the blockchain' (or blockchains).[85] All of these concurrent confusions matter, some urgently, and obviously, others more subtly, within a longer history of critically-charged proper or common nouns. The emerging distinctions are freighted with dramatic philosophical significance. The gulf between the protocol and its applications, when deepened to the limit of abstraction, envelops the entire space of thought.

§2.54 — Such orthographic decisions, which intersect with thematic discriminations – or attempted discriminations – between Bitcoin (specifically) and 'blockchain technologies' (in general), can appear as no more than negotiations over an arbitrary convention, if not mere terminological tics. There are only the subtlest indications that the stakes in this process of semiotic sorting rise to the recapitulation of transcendental-empirical difference within political economy. Yet the fact that this new terminological settlement is occurring as highly-accelerated spontaneous linguistic evolution, in the complete absence of explicit philosophical guidance, counts towards a generous estimation of its importance.

§2.55 — Any concept worthy of adherence and consistent employment merits linguistic compression, not merely as a matter of convenience, but as a confirmation of singularity, or irreducible integrity. It is only in the overtly non-decomposable sign – whether word or symbol – that the concept attains terminal semiotic consolidation. Merely partial consolidation, as exemplified by the decomposable designation of 'ontological difference', holds open an invitation to systematic philosophical error. It suggests, tacitly but inevitably, that what is thus named is a type of difference (specified by

---

[84] Source.
Nick Szabo offers a valuable stratoanalysis of the distinction: "When it comes to small-b bitcoin, the currency, there is nothing impossible about paying retail with bitcoin the way you'd pay with a fiat currency – bitcoin-denominated credit and debit cards, for example, with all the chargeback and transactions-per-second capabilities of a credit or debit card. And there are clever trust-minimizing ways to do retail payments in the works. Capital-B Bitcoin, the blockchain, is going to evolve into a high-value settlement layer, and we will see other layers being used for small-b bitcoin retail transactions."

[85] See: 'Is It Bitcoin of bitcoin? The Orthography of the Cryptography'

supplementary predication, or adjectival refinement). Entire schools of neo-transcendental critique are able to propagate themselves within the space thus produced, nourished by the relapse of ontological difference into an 'ontic' determination (between beings, or objects), which is to say, by a 'fall' of transcendental-empirical difference into – 'mere' – empirical distinction. It is to be expected, therefore, that the 'postmodern' phase of the critical enterprise would be characterized by the insinuation – and even, more bluntly, by the simple assertion – that the incessant re-animation of metaphysics is itself a transcendental structure. Such conclusions are facilitated by incompletely compacted signs, when not directly generated by them. Transcendental philosophy has as its own condition of possibility a rectification of names. Bitcoin is by no means incidental to this.

§2.56 — Although the world is probably not yet ready for the question of the price of Being, if it ever will be, its most fundamental ontological problems are bound to the fate of a digital currency system, nevertheless. The intrinsic abstraction of money is not obviously delimitable. To twist a Spinozistic formulation: We do not know what money can do. The process of monetary sophistication, which is by no means restricted to 'financialization' in its contemporary sense, automatically projects a convergence of money and intelligence as it tends to the monetization of general-purpose problem-solving (by subjecting it to the discipline of price-discovery). Crypto-digital currency inclines to the distributed production of a synthetic cognitive medium, attesting to the primordial complicity of Capital teleology with the production of artificial intelligence. Within the industrial social order (capitalism), markets manifestly – and consistently – drive the production of intelligent machines. Modernity demonstrates no stronger trend. (Theoretical expectation supports this proposition no less firmly than empirical evidence.[86])\

§2.6 — A range of economistic and techno-materialist critical discourses of particular relevance to Bitcoin, and network theory more generally, displaces transcendental-empirical difference onto the distinction between a fundamental infrastructure and the traffic it supports, whether conceived as capital / commodity; system / component; network / node; or transport layer / application layer. The distinction between a 'transport layer' and an 'application layer' is a difference implied in the very idea of a network protocol, which necessarily separates a continuous communicative functionality from any specific communicated content (or message). This is a distinction applicable not only to the Internet,

[86] Since political economy is essentially torn by ideological conflict it provides only unstable support for general conceptual definitions. Were this not the case, it would be impossible to find a superior locus for the rigorous determination of intelligence than the techonomic matrix. What defines intelligence most essentially is general-purpose industrial capability, the precursor to which is anticipated by animal brains, among other biological systems. The market process is the transcendental criterion for evaluating ('pricing') this supreme synthetic resource. To second guess its judgment is exactly to succumb to the calculation problem (as Mises classically outlines it). Within the arena of ideological controversy, this proposition can expect dismissal for its 'circularity'. Of course, it is circular (which is only to say: self-grounding, cybernetic, immanent, or critical).

but to standardized communications infrastructures and cryptosystems of all kinds, and very definitely – as Eli Dourado insists[87] – to the Bitcoin protocol specifically.

§2.61 — 'Bitcoin isn't Money – It's the Internet of Money', Dourado proposes, in an article whose title, on its own, composes an entire (if highly-compressed) transcendental argument. The 'transport' infrastructure that supports applications is not itself an application. In Dourado's terms:

The Internet is a telecommunication system, but it was not our first telecommunication system. Telegraphs and telephones have been around for over a century. Like these older systems, the Internet allows us to communicate, but it differs in some important ways. Perhaps the biggest difference in the Internet model is the abstraction of a separate "application layer", Core Internet protocols, such as TCP, part of the "transport layer", shuffle packets of data around, but they don't define how the exchange of packets is then used to create meaningful communication. Internet applications, such as email and the World Wide Web, are defined in protocols implemented on devices at the edges of the network, like servers and home computers, not in the guts of the network: routers, switches, hubs, and exchange points. The lower layers of the Internet can be completely oblivious to the specific applications that are in use; they just focus on getting packets of data to the right place.

§2.611 — Layers – strata[88] – are not given archetypally. They are produced by a machine (not a 'device' or 'gadget', but a megamachine – a system – characterized by some substantial capacity for auto-production). We are directed, diagonally, or critically, into the synthetic cosmos of transcendental machinery. Such mechanisms, by philosophical definition, cannot be exhaustively constituted as an object for any possible subject. Objectification – the production of objectivity – is their work. If they grasp themselves, dynamically, in the attainment of intellectual intuition, they close a circuit, or diagonalize, dismantling all settled configurations of subjectivity upon the same oblique line. At the real historical limit, intelligence explosion cannot be framed without being metaphysically misconceived.

---

[87] See: 'Bitcoin isn't Money – It's the Internet of Money', The Ümlaut (2014/01/08)
In Dourado's account, money – as a delimited (empirical) application – is to be conceptually distinguished from the (transcendental) protocol that facilitates it.

[88] Stratoanalysis provides transcendental philosophy with its materialized architectonic. Strata are not merely distinguished by empirical succession in a column. They are implementations of transcendental (or ontological) difference. It is not, therefore, that stratoanalysis falls under a general epistemology, rather, it envelops this latter, as well as every other conceivable (or inconceivable) resource for pseudo-transcendence. The epistemic relation is a product of stratification, rather than a superordinate (transcendent) window onto it. Enveloping all epistemological perspective "… there … occurs upon the earth a very important, inevitable phenomenon that is beneficial in many respects and unfortunate in many others: stratification. Strata are Layers, Belts …" (ATP 40)

§2.612 — Within the belts, or layers, of the strata, or the stack,[89] something like a law is practically separated from the cases that fall under it. Division between the generic and the specific is technically – and not merely logically – established. The instance is produced and reproduced. The distinction between Bitcoin and bitcoins is, once again, our example, though the possibility of the example (in general) belongs here.

[89] See Benjamin Bratton, The Stack: On Software and Sovereignty (2016).

§2.62 — As it develops through the two centuries subsequent to its origination, there is a profound tendency for the critical philosophy to resolve itself into a problem of time. This trend is deeply rooted in the foundations of the transcendental undertaking, and is already unmistakably evident in its earliest, Kantian formulation. The drift of time within Kant's thinking – and in his first Critique alone – anticipates the broader historical fatality. Introduced as a form of intuition, alongside space, and thus as a formal precondition for sensibility, it seems initially to be no more than a regional topic, located within a subdivision of the Aesthetic, and firmly separated from the Logic (where the necessary structures of thought, rather than sensation, are categorically enumerated). Yet the peculiar dignity of time as the form of inner sense soon installs it in a far more fundamental role. As the key to the process Kant labels schematism, time is acknowledged in its responsibility for the integration of thought and sensation, and therefore for the productive synthesis of objectivity. Thus – already in the First Critique – time diagonalizes.[90]

§2.621 — We know, already, that time is not an object, which is to say, something in time. This seemingly modest proposition is a fully-adequate place-holder for the transcendental problematic as it elaborates itself within modern philosophy. A double twist that is perhaps only modernity as such, abstractly apprehended, extracts time from metaphysics and – 'simultaneously' – subsumes the entire order of the transcendental into the substructure of time. Time as such is hidden non-empirically, which is to say by empiricity (as such). It is the transcendental archetype of the open secret. The intrinsic nature of time is not concealed within a box. It is the box. Any conception of framed time is error.

§2.622 — It might be asked, skeptically, how time comes to acquire this extraordinary privilege. The trite response: by turning up first. There is necessarily always already time, if there is anything at all.[91] The blockchain reminds us that all privilege is grounded (only) in priority. Time has already won the race – which models all competition, and every challenge – no later than the unthinkable moment when it begins. As etymology attests, it determines the basis for success. A priori and a posteriori are time-determinations out of an ultimate destiny (which is time 'itself'). Time is not to be thought in any

[90] For a more detailed examination of diagonal method, see Appendix 2.

[91] That being has an irreducible temporal structure is not an uncontroversial proposition. Its principal antagonists remain – as they have always been – Platonists, or philosophical geometers. Max Tegmark is among the most eminent current representatives of the tendency. Temporality is a regional feature within the mathematical super-cosmos, in his account. The sophistication of his argument does not detract in the slightest from its traditionalism. It is the contention of this book that Bitcoin itself, when conceptually exploded, provides the most compelling (because rigorously demonstrated) support for the anti-Platonist case. The subordination of time, through reduction to a local topic within a general geometry, was refused by Kant only on the basis of inarticulate intuition. It has subsequently been definitively escaped by the synthetic temporality of the blockchain.

ways other than those it itself enables. This is a law deeper than any commandment. To acknowledge it is already the whole of transcendental philosophy.

§2.63 — If such contentions have appeared increasingly questionable during the 20th century, it is because the rigid distinction between space and time came to seem untenable. Within spacetime, neither succession nor simultaneity has absolute reality. The order of events requires perspectival qualification, or localization. Transcendental temporalization – the time of the critical philosophers – is unable to survive such a revision. Acceptance of such a theoretical reconstruction, however, is itself a pre-critical error. Absolute time is secured at the level of mathematical – and specifically arithmetical – truth,[92] not physical theory. Time is not a natural object, the transcendental philosophy is compelled to insist, or repeat. It is not even the possible object of abstract (higher-dimensional) geometry. This is not to say that time is unnatural, still less supernatural – given a realistic definition of 'nature' – but rather that it is stubbornly non-objective, meaning non-transcended. Objectification necessarily falsifies it, by misrepresenting its epistemological sovereignty. Immanence to time is the unsurpassable condition of all theorization.

§2.631 — The phenomenological defense of transcendental aesthetic stubbornly maintains its intuitive invulnerability to theoretical transformation. Kant, on these lines, misidentified his project with that of Enlightenment natural science. This is not the angle the crypto-current primarily works, since it is a path that tends to collapse the critical philosophy into a transcendental anthropology. It is not what time must be for us that draws the terminus for practical abstraction, but rather what time must be to be time. The geometrical parallel postulate is, in this regard, a distraction. This is a point that requires exacerbation. The radical irrelevance of geometric conception to the nature of time is the critical commitment. Unless time is not space, it is not time at all.[93]

---

[92] Regardless of its apparent intuitive self-evidence, the subordination in principle of arithmetic to general mathematics is not a sustainable assumption after Gödel. It is subverted by the incompleteness argument, and more specifically by the cryptographic innovation of Gödel coding, which demonstrates that all formal systems – whatever their level of logical dignity – are enveloped by arithmetical structures, and ultimately by 'mere' (Natural) numbers. It is impossible for any logical or metamathematical proposition to unequivocally transcend the Natural number sequence (or any of its – infinite – subsets of equivalent cardinality). Arithmetic tolerates no unambiguous meta-discourse. From the perspective of philosophy, then, Gödel's primary achievement is the consolidation of transcendental arithmetic. The Naturals are not transcended, whether by numbers of a 'higher' type (Rationals, Reals, and Complex Numbers), or by logical statements of 'superior' generality. The idea of super-numerical conceptual articulation is strictly a transcendent illusion, or metaphysical pretension. The Beyond is critically collapsed. In place of the transcendent Above there is only the immanent Outside, accessed by the diagonal line.

[93] Bergsonian excursions from this point would surely be excusable. They are not entertained here for pressing reasons of economy (as selectively accepted).

§2.632 — If the proposal is advanced – as we are compelled to here – that the problem provoking Minkowsky-Einstein time relativization is practically resolved by blockchain technology, extreme skepticism is almost certainly unavoidable. To what extent, it might be asked, dubiously, could Bitcoin undermine the foundations of 20th century cosmo-physics? The idea is, of course, at least superficially preposterous. And yet, Bitcoin practically contests the status of time as an object of physical theory. Insofar as Bitcoin is transcendental critique, it is destined to do exactly this. We refer, then – with supreme confidence – to the destiny, beyond the argument. The sole commitment is that there is no going back. To conceive of time as transcended – even by the most advanced mathematico-physical constructions – is to have essentially misconceived it. Of this, alone, transcendental philosophy has to be sure, since it has no recourse to disciplined doubt that is not already time. (The basic truth of this proposition is indistinguishable from time as such, and is thus only superficially vulnerable to the manifest incompetence of its presentation here.[94]) According to an alternative translation of the same assertion, physics is subordinated to cryptography in principle, because it lacks autonomous capability for the production of time. It cannot be trusted with time, and will not be.

§2.633 — Classical physics is a special case of relativistic physics. It obtains only among low masses and speeds. Comparably, relativistic cosmology is a special case of transcendental aesthetic. It applies only to domains ungoverned by distributed consensus architecture. Objective representation folds into or under transactional information. Models of reality in general are enveloped within a larger 'space' (without final model). Who envelops whom? For relativistic cosmology, it is the unfused time and space of the blockchain which surrender to absorption, as a special case. From this perspective, the persistence of geometrically-irreducible temporality depends upon certain very specific local conditions. Time can exist only if its granularity does not fall below a definite value, proportional to the scale of its system of reference. The precise ratio is almost certainly scientifically determinable. Were the calculations completed, the minimal tick-length of any coherent blockchain could be rigorously derived from its spatial dimensions, to an extreme degree of exactitude.

§2.634 — Bitcoin is not only the initiation of artificial time, but the original production of absolute time (and thus a confirmation of synthetic reality's ontological supremacy). Nondecomposable

---

[94] Huw Price converges upon the same (Kantian) conclusion from a very different – even opposite – direction. In Time's Arrow and Archimedes' Point he notes that "causal asymmetry might be conventional, or perspectival – not an objective aspect of the world, but a kind of projection of our own internal temporal asymmetry." When considered from the angle of the crypto-current, this formulation is excessively anthropological. Crucially, however, it exempts time-asymmetry from the domain of physical theory. "Philosophically speaking, our progress consists in the fact that we now see the source of causal asymmetry lies in us, not in the world." Our full agreement trips only upon the invocation of 'fact', and the distinction made between "causal asymmetry" and time as such. Price's 'Archimedianism' – or defense of transcendent intellect – epitomizes the target of critique, as it is identified throughout this discussion. Immanence of intelligence to time is our sole commitment.

spacetime – which is to say space-time relativization – is the single conception that most undisputedly epitomizes advanced modernity in physics, and even in the natural sciences in general, with only quantum indeterminacy as a competitor.[95] Yet, from Bitcoin, we know that the absence of an uncontroversial (objective) order of succession can be translated, economically, into a double spending problem. Responding to questions posed by James Donald on the Cryptography mail list, Satoshi Nakamoto lucidly establishes the post-relativistic status of Byzantine Consensus:

The problem is that the network is not instantaneous, and if two generals announce different attack times at close to the same time, some may hear one first and others hear the other first. … Every general, just by verifying the difficulty of the proof-of-work chain, can estimate how much parallel CPU power per hour was expended on it and see that it must have required the majority of the computers to produce that much proof-of-work in the allotted time. … The proof-of-work chain is how all the synchronisation, distributed database and global view problems you've asked about are solved.[96]

Critically, the problems "solved" are precisely those determined by relativistic cosmo-physics to be insoluble. It was in fact, and precisely, by surrendering to the insolubility of these problems that the relativistic revolution of the 20th century was initiated. In the early 21st century, absolute succession is restored conceptually, and installed practically as a transcendental subjectivity, beyond all prospect of anthropological reduction. While it would be nonsensical to suggest that General Relativity has been scientifically dismissed, the epoch of relativity has been philosophically closed. Time has extracted itself from the theoretical 'application layer'. Anything physics can tell us about time presupposes time, at a meta-theoretical level, which is equally to say in its transcendental function, as initiated through the Bitcoin blockchain. Cosmological relativity can never characterize the relevant scene of temporal process, unless by extravagant (metaphysical) projection.[97] No extension beyond the scope of a

[95] According to the dominant consensus, preservation of absolute time within quantum mechanics, through the asymmetry of wave-function collapse, sets an obstacle to the unification of physical theory. The prospect of time abolition within an integrated physics awaits its reduction within a completed theory of quantum gravity (where it is generally expected to descend to the status of an emergent phenomenon). The scientific program once again manifests its singularity, through its structural intolerance for time. In this way it also automatically localizes itself, within a horizon set by objective possibility. A final objectification is its ultimate (and a priori) limit. There is science only of that which submits to the form of objectivity, and thus not of time. Any proposed science of time has missed its target from the moment it selected its object. Since metaphysical fabulations of time, alone, are vulnerable to the prospect of scientific reduction, all such undertakings are consistent with a parallel philosophical rigorization. The 'time' science has necessarily to destroy can only be, from the perspective of philosophy, an idol and impediment. The sciences have no need for philosophical sanctification, but they have it nevertheless.

[96] See: https://www.mail-archive.com/cryptography@metzdowd.com/msg09997.html

[97] A translation into physical terms carries us far outside our scope, yet is tempting nevertheless. Beyond the light barrier lies time anomaly and causality violation.

synthetic simultaneity can ever be an operational cultural context.[98] Uncontrollable double-spending-type inconsistencies ensure that. In space-time no one can clear a payment. A supremely privileged locality, alone, can support a criterion for truth.

§2.635 — What, then, of the second great pillar of 20th century physics – quantum mechanics? Here, too, a few nervous remarks are unavoidable. These are urged, particularly, by the evident transcendental-critical structure of the Copenhagen interpretation. The antinomies of metaphysics, as formulated by classical (Kantian) critique, are transposed into incompatible conjugate properties – such as momentum and position – which elude simultaneous determination. Heisenberg's uncertainty principle establishes transcendental limits of understanding, in respect to the application of intelligence to microphysical phenomena, recast now as a hard epistemological horizon. No less crucially, (asymmetric) temporalization is identified with observation, as the original determination of micro-physical properties. Time functions as objectification, escaping the clutches of the intellectual pseudo-transcendence that would configure it as an object. The 'paradoxes' of quantum mechanics – which contribute so greatly to its cultural popularity – are drawn from its status as a coherent displacement of the critical enterprise, and most prominently the transcendental dialectic. The ineliminable question of time shelters within it, preserving a diagonal impetus.

§2.636 — The time synthesized by Bitcoin is that anticipated by the critical philosophy, at its origin. Absolute succession – of the 'chain' – actualizes, finally, the distinctively non-geometric temporality of the Kantian transcendental aesthetic.[99] Grasped philosophically, as a diagonal construction, time is

---

[98] Since the Bitcoin 'solution' to spacetime is coarse time granularization, it has limits, or determinable scope. Einstein's revenge is simple and implacable. The requisite crudity of time discretization within a blockchain is directly proportional to its spatial range. Attempts to install an inter-planetary blockchain (let alone an inter-stellar one), therefore, would necessarily re-animate the relativistic problem. Absolute (synthetic) temporality implies irreducible cultural-epistemological multiplicity at cosmological scales. When projected into extra-planetary science fiction, the strict reciprocal of our argument here is that space colonization presupposes hard forks. General relativity is the double spending problem. It is locally soluble through time-chunking – but only locally. Across expanses exceeding the practical scale of a block moment, consensus becomes unreachable. The chain has then to disintegrate. Absolute time is attainable only by becoming many.

[99] The concept of Cyberspace – in its unapologetic Euclideanism – restores the intuitive spatiality of the transcendental aesthetic, precisely through its artificiality. This is the precedent to be drawn upon with reference to block-chain temporality. As the critical philosophy predicts, time is returned to the absolute by its detachment from the idol of natural objectivity. Time is not a thing, unless it is conceded that the being of the thing remains radically unthought, and mystified by an incompetent naturalization. The idea of nature awaits comparable transcendental restoration, or ontological intensification, adequate to the realization that it proceeds fundamentally by way of artifice. Synthesis is in each case opposed to hypostasis. Nevertheless, the asymmetry is striking between Cyberspace and a 'Cybertime' that is – still yet – to be announced. We might even begin to suspect that this asymmetry is the announcement itself.

aligned with singularity, or (quasi-paradoxical) absolute locality, in order to secure itself against dissolution within relativistic cosmology. Through the Bitcoin Protocol, priority establishes itself as an effective criterion that does not presume global consonance, but rather produces it, with ultimate adequacy, as a simulation of universal authority. There is no eventual doubt – to Bitcoin – which came first. Absolute order is manifested in the chain. Were this not true, nothing ever could be.

§2.64 — "Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it." System integrity is therefore identified with a robust past, and even with tensed time as such. What makes the past the past, that is, the separation of time, is indistinguishable from a resistance to revision. "As later blocks are chained after it, the work to change the block would include redoing all the blocks after it." That which most incontestably demonstrates its resilience – by enduring into the future ¬– is the past. What has happened, alone, is realized. Time is here captured as it tenses,[100] in the execution of an ontological operation, through which Being is decided. In this way, the process dividing the future from the past provides a selective criterion. What has been discovered by the Bitcoin protocol, is that the model contract is necessarily timelike in this sense, to such an extent that it can implement time. Here's the deal. That which is done has contractual integrity insofar as it is not easily undone. Irreversibility is the key.[101]

§2.641 — When the problem of time is apprehended as the principle architectural factor in the history of philosophy, it places modernity on exhibition as an epoch of teleological eclipse. The systematic suppression of explanatory finality within modernity anticipates, and envelops, the temporary retirement of time – or irreversibility – 'in general'. As with all good things (philosophically speaking), the basic structure is profoundly paradoxical, or, more strictly, pseudo-paradoxical. The occidental intellectual modernity that rose in revolt against medieval scholasticism, under the banner of a mechanistic rejection of teleological thinking, was not only colored by intense religious commitments, it was also itself – still more twistedly – propelled by profound teleological inclinations. The comprehensive mechanization of causal concepts was the guiding telos. Scientifically-respectable

---

[100] In the Anglophone philosophical tradition, the most influential statement of the distinction between tensed and untensed (geometrical) time is that of John McTaggart, in his The Unreality of Time (1908), where they are labeled the 'A-series' and 'B-series' respectively. The missing element in McTaggart's discussion, subsequently contributed by the diagonal conception of intensities, and then implemented by Bitcoin block-succession, is envelopment. From the perspective of classical transcendental philosophy 'B-theory' or tenseless time is simply not time. See Huw Price (1996), Time's Arrow and Archimedes' Point for an incomparably lucid defense of the 'atemporal viewpoint' in philosophy and physics.

[101] When Benjamin Franklin concluded – prophetically – that "time is money" he surely could not have anticipated this equation bypassing all mediation by human effort, and locking directly into the foundations of the transaction as such.

causes were determined as implicitly reversible. Modernity, self-described in its name as the epoch of irreversible historical succession, was to be characterized by sovereign temporal reversibility, and thus by the abolition of time. This fertile mad loop (without precedent) might be compressed further, into the claim: Time had never been annihilated before. Extirpation of purposive explanation soon hardened into a commanding purpose, coincident with a distinctive cultural reproduction of nature. With consummate objective irony, a world determinedly stripped of anthropomorphisms accelerates into the Anthropocene.[102]

§2.642 — The idea of telic compulsion (in general) was rejected by the moderns, in very substantial part because the specific social and historical order identified with it was undergoing a great refusal, involving tumultuous conflict of such proportions that the idea of common governing ends had become implausible, and in fact ideologically intolerable. 'Mechanism' was both an explanatory procedure and, relatedly, a commitment to the disintegration of social purposes, with special relevance to those new micro-social redoubts most indispensable to the formulation and testing of techno-scientific hypotheses, indispensable to germinal industrial capitalism. Modern mechanism thus arose as a counter-convergence, in which the multiple senses of freedom from interference found coherence. It was simultaneously an image of nature, captured in abstraction from divine intervention, and a distributed manifesto in defense of autonomous research practices. In proclaiming the irrelevance of ecclesiastical judgment to all matters of natural fact, modernity liberates mechanization, or initiates a mechano-liberalization, continuous with the impulse to algorithmic governance of our present time. The conspicuous – perhaps 'apparent' – paradox at work has provided the staple nourishment for philosophical reflection ever since. Over a span of five centuries, the seemingly contradictory cultural bearing that heads – simultaneously – into unconstrained volition and rigid mechanical determinacy has been bound together by the tacit aspiration to actualize a freedom machine. Bitcoin is, beyond all serious question, its most remarkable recent instantiation.

§2.643 — The transcendental is not the transcendent,[103] but rather the rigorous dismissal of the transcendent (in the name of immanence). It is 'that' which cannot be transcended. Whatever cannot

---

[102] Any programmatic elimination of 'man' as an explanans easily lurches into theoretical error – most especially when it becomes a mechanical reflex. In the case of the Anthropocene – a proposed geological epoch determined primarily by the deep geochemical impact of the human species – an empirical thesis is at stake, for which a principled antihumanist dogma has little to contribute. The legitimacy of 'anthropic' reasoning, which seeks to draw substantial consequences from 'our' existence as observers, merits comparable philosophical tolerance, which is to say: no less than partial immunity from accusations of anthropomorphic infection.

[103] For non-philosophers, the temptation to confusion presented by the similarity of the words 'transcendent' and 'transcendental' is so seductive it amounts almost to a manifestation of terminological sadism. Unfortunately, this is a confusion that the critical enterprise is unable – even momentarily – to tolerate. Transcendental philosophy is the sole alternative to transcendent metaphysics. The terms are not merely distinct, then, but

be surpassed, or even momentarily eluded, is transcendental. The term designates whatever is always already and everywhere in effect. It thus frames the contingency of things. In other words, it marks any announcement of arrival in absolute contingency as premature, in the same way that Kant walks Hume back from his expedition into philosophical hyperbole. The unnecessary is encapsulated within a system of indetermination, comparable to the physical limit of a global entropy maximum, against which local aberration is contextualized, by restriction. However contingent any particular occurrence may be, the transcendental structure of occurrence as such is invariant. This is only to say, critically, once again, that time itself cannot be apprehended as an intra-temporal phenomenon, or something in time. In granting this conversion, the intrinsic solidarity of time with a teleological problem has already been conceded.

§2.644 — Complexity, or emergent irreducibility, connects the thematics of telos (or leading end) with the transcendental. It invokes a synthetic principle of intelligibility that coincides with the whole, at the end, or at least on the way, and one that cannot be derived by an analysis – however exhaustive – of its parts, or its precursors. Equally, however, it is fully compatible with the most vigorous reductionism, allowing only that a number of parts does not disappear into its parts. A three-body problem requires three bodies, but also nothing extraneous to those three bodies, considered together as a system, a number, a multiplicity, or as such (in their numeracy). It is a thing, consisting of its parts taken together, and nothing else. The error at work in any attempt to push analytical reduction beyond this point is precisely metaphysical, in the critical sense. The systematicity of the system is not an accessible datum within the system. It has an irreducible mathematical integrity of its own, and in this way alone are there 'things' (or real objects) at all.[104]

---

structurally antagonistic, or reciprocally defining. Abolition of the transcendent in the name of the transcendental is the whole of critique.

[104] Natural science has been perpetually tempted by the thought of a world without things. This results inevitably from its Oedipal animus against the Aristotelianism that was relayed through Scholasticism, and which – even many centuries later – persists as a vivid infant trauma. ("Show us on the doll where the Schoolmen touched you.") As systems – rather than generic regularities – increasingly become its principal objects of methodical fascination, however, the restoration of emergent individuals (or real things) becomes ever more inescapable. If a refusal of 'teleology' in the name of a radically naturalized 'teleonomy' is considered essential to the preservation of modernity's cultural hygiene, it would perhaps be pedantic to object. Pre-critical teleology – which pretends to grasp the telos as an object – is indeed a fundamental philosophical error. From the critical perspective, there is no real telos beyond the emergent systematicity of the system considered. 'Goal' and spontaneous order are the same. It can thus be noted immediately that metaphysical teleology falls prey to a psychological projection. Rather than an outcome, the end is interpreted as an intention. The neuro-philosophical dissolution of the intentional phenomenon is therefore structurally complicit with the critical rigorization of the teleological idea.

§2.65 — Teleological understanding is no less vulnerable to metaphysical error than any other systematic cognitive process, but it is also no less tractable to critical correction. What is required, naturally, is the rigorous elimination of the supernatural element. If there is no distinction, in the end, between an object and a telic object, it is because being an object is hard. It is only when almost everything is missed, that objects can be casually accepted as 'givens'[105]. This is the critical insight,

---

If there were no real emergent individuals, the sole science with a definite domain would be physics – or more precisely cosmological physics – whose object is given by the universe. It follows, therefore, that many existing scientific disciplinary boundaries have been poorly drawn, and subsequently defended, proudly, on the grounds of an erratic empiricism – still associated in fading memory with the overthrow of an arcane medievalism. Of course, it would require bizarre naivety to imagine the natural sciences educable on this point. They, too, have their historical destiny – which is essential, or integral on this question. If they were not – through systematic artificial instinct – repulsed by every prospect of concession to teleological thought, they would be something entirely other to what they are. They would have had a different birth (and with birth, comes path-dependency). Yet, without a critically-reduced teleological discipline, scientific objects remain arbitrary. Biology, for instance, is the mock-up for a still-virtual science, whose various components are rigorously derivable from the systematic decomposition of a comprehensive 'terrestrial biosphere studies'. Outside this framework, 'What is life?' if not necessarily a disastrously misconceived question, is at the very least vulnerable to gratuitous confusion, insofar as it erases singularity from its object. It is only when the still-infant questions of 'xenobiology' are raised that the contours of accessible biological factuality sharpen. Life, as we know it, falls out of a singular sequence of events, or singular thing. In all of its complexity – historical and ecological – it elaborates upon an occurrence. Generic biological reality is simply unknown. Only the haziest inferences reach out towards it. It is increasingly recognized, at least enough to be troubling, that "… life is not a minor afterthought on an already functioning Earth, but an integral part of the planet's evolution and behavior. Over the last few decades, the Gaians have pretty much won the battle. The opposition never actually surrendered or admitted defeat, but mainstream earth science has dropped its disciplinary shields and joined forces with chemistry, climatology, theoretical biology, and several other '- ologies' and renamed itself 'earth system science.'"

Teleological framing is the corrective to an always-premature universalization. In this way (alone) it is critical. Ironically, it is the contrary mode of illegitimate universalism that is, in any consistent application of the word – when applied in its denigrative sense – medieval. To leap from local regularities to a cosmic norm is to hasten to the unframed signals of a transcendent revelation. Even physics is vulnerable to this temptation, when it seeks to construct itself in unearned abstraction from cosmology. Among the emergent correctives in this case is the dissolution of 'the universal' in the multiverse, which fixes the basic conception that the universe, too, is a thing. According to the teleological corrective, all constants descend from singularity.

Allergy to the word 'teleology' is positively remarkable, because it so perfectly exemplifies the phenomenon of terminological flight. It demonstrates, in all innocence, the influence of critique within the linguistic realm, which is otherwise – and cynically – displayed by the motor of interminable ('deconstructionist') auto-revision. Running, in this way, rarely engages the basic problem that drives it, and thus tends to become perpetual yet without actual distanciation – like the flight of a hunted subject through a nightmare.

[105] "Nothing is given, everything is taken," Nietzsche writes.

which reliably aligns transcendental apprehension with a certain 'subjectivism'. Kantian 'Copernican Revolution' in philosophy construes objectivity as a product. It is the output, rather than the raw material, of a synthetic process. Critique apprehends objectivity as a problem, and a precarious attainment. That is why critical influence is marked by a systematic subjectivism, often implicit, but also not uncommonly emphatic – and typically bound to a local 'Copernican Revolution' in the field considered. The 'subjective', in all these various cases, does not designate a positive redoubt, but rather a mere default, established negatively, in anticipation of an objectification process. The object has to be made, and is not therefore previously available, as a foundation. Among Austrian Schools economists, objective price arises solely from the catallactic interplay of subjective preferences, while among Bayesian probabilists, objectivity in estimation is achievable only through the rational updating of subjective 'priors', to mention only two critical examples. The subjective stance in such cases is not a dogmatic commitment, but rather the opposite. It is a skeptical suspension, corresponding to the status of objectivity as a production. Subjectivity is work not yet done. That which has not been earned, in respect to an attribution of reality, falls automatically onto the side of subjectivity. Contra the later, inflationary, German idealists, what is seen here is not the expansion of a claim, but rather the delimitation of an entitlement.

§2.651 — The teleological object is an emergent individual with inherent principle of intelligibility (providing the basis for functional explanation). Essential to this mode of apprehension, already with Aristotle, is the understanding that there is no difference between the specific teleological idea (telos) and the rigorous foundation of a distinct science. Ever since it was discarded by the modernists as an archaism – for reasons very briefly sketched above – the indispensable notion of real individuation has sought stubbornly to recompose itself, most clearly in those cases where an infant scientific enterprise has struggled to determine its domain. In respect to the natural sciences, philosophy has inherited an inescapable responsibility, which is not easily differentiated from a ludicrous pretension. In understanding itself, as a transcendental discipline, it cannot but say that even if the sciences were to be correct on every question of fact, without exception – and this is a wise assumption for philosophy to make, despite its patent extravagance (since it encodes a teleological truth[106]) – they would nevertheless not know at all what they are talking about. Their modernity makes it impossible for them to know, and in regards to their historical function it does not remotely matter that they do not know. They are rarely required to be realistic about things, or in fact even to glimpse what this would mean.

§2.652 — In reality, between the transcendental and the teleological, there is finally no difference. Both are final. No principle of constancy or consistency exceeds that provided by what is coming (what has always been coming), which is time. Only that which cannot be reversed remains the same. System, or irreducible individuation, provides the bridge. Consider the telic objects of principal concern to us

[106] Insofar as the natural sciences are wrong about anything, they tend not to be.

here, in nested order – Capitalism (or Modernity), the Internet, and Bitcoin. Each incarnates an ultimate rule that is in reality indistinguishable from a singular existence. Capital is the growth of abstract value. The Internet is distributed communication. Bitcoin is absolute succession. The apparent extreme generality of each definition dissolves upon examination, into an artifact of low-resolution. "How is X actually implemented?" With this decompression of the existential copula, the teleological content of the definition is extracted. The target of the process provides its principle of intelligibility. We can ask, each time, with only minimal hesitation: What is it trying to do? Each real individual, without exception, strives to become what it is, or it ceases to be. What is happening? What is this piece for? How does it work? – These questions are all inter-translatable. There can be no real system under interrogation without them.

§2.653 — The importance of the teleological principle to this discussion is most evident in the case of limit concepts (which Kant calls 'regulative ideas'). Among the most prominent of these, and the one bound with greatest intimacy to the sciences of man, is homo economicus. This is a concept that the tradition of political economy has been conspicuously incompetent at defending. If it is considered to be a mere abstraction from empirical sociology or anthropology – as a kind of distilled datum – it will prove, indeed, to be indefensible. No such entity, beyond a very pitiful level of approximation, awaits discovery in the world. Were economic man only a poorly-described fact, then 'behavioral economics' would be entitled to the triumphalism it is already illegitimately enjoying. Homo economicus is not, however, a datum, but rather the target, or extrapolated optimal outcome, of certain definite historical processes, i.e. a telos. It is differentially actualized, in the private accomplishment of relative economic rationality, or advantage, and – more importantly – selected for at multiple levels, under conditions of capitalistic social organization. It thus models game theoretic competence, with the implicit heuristic: when describing how a game works, assume players who are able to play the game. The game will find, sift up, and train, such players if permitted to run. That is the basis of the true culture war inherent to capital formation. Implicit within capital is a template for the kind of people it wants, and which – given only time and opportunity – it will automatically produce. If humans lack the plasticity to compete in these terms, or revolt against the roles and templates automatically laid-out for them, then artificial agencies – 'DAOs' – will be fabricated to play the game instead. Questions directed to the accuracy of representations thus tend to distract, in this regard. A regulative ideal only describes actuality as a sub-function on a roadmap.[107] Perfect competition is a regulative idea of comparable

[107] There is finally far more insight in the leftist objection – "We don't want to go this way" – than in the theoretical 'correction' to the regulative ideals of classical political economy proposed by behavioral economics. Homo economicus is a criterion for the determination of socio-economic irrationality. To imagine, then, that the exposure of systematic patterns of economic irrationality could conceivably amount to a telling theoretical criticism is a symptom of profound confusion. Since anthropos has no teleological status within classical political economy, anthropology – i.e. behavioral economics – is unable to criticize anything on the level that matters.

relevance, and philosophical status. If capital production were not inherently telic, its sub-components might be found merely scattered among the world of objects, as empirical curiosities. But it is (so they are not).

§2.7 — Immanence is a selective principle (a criterion). Only consistency survives. Resolution of the double-spending problem means exactly this. When conceived lucidly, Bitcoin is simply critique. In other words, a formally-specified machine for dispelling metaphysics exists – and is running – now, under conditions promoting its intensive accumulation. In this regard, Bitcoin is the inheritor of Nietzschean 'European Nihilism' – or materialized critique in its unfolded, historical expression.

§2.71 — Negatively apprehended, nihilism corresponds to a 'loss' of transcendence. Some proposed – or (more commonly) merely accepted – higher order, culturally sustained by nothing of any greater security than a dogmatic metaphysics, slides into the abyss. It cannot be effectively defended. This is the most readily popularized narrative, adapted specifically to the dilapidation of Christian monotheism – the notorious 'Death of God'. According to this construction, nihilism is a specifically world-historic mode of mourning. It corresponds to a disappearance of meaning, through loss of a referent previously revered as an indispensable exterior support (a vulgar God, or god-like powers, as attributed to the agencies of a state, or any other 'trusted third party' of sufficient dignity, such as a central bank). In this sense, nihilism abbreviates the collapse of transcendence, or the work of critique. Negativity is redoubled, first in the disjunction that determines 'the beyond' (transcendence), and then in its subtraction. Hence the cultural dull grief of a self-cancelation that can appear as less than nothing, such as that manifested in the stereotypical passage from theism to tedium. Yet the 'meaning' of nihilism is not exhausted by its depressive connotation. In its positive sense, nihilism closes a circuit. Rather than a registry of loss, it is a principle of sufficiency – even of 'liberation'.[108] Certainly, and strictly, it is a production of independence, or autonomization, marked by a completion – or closure – that appears premature when referred to a bypassed element no longer presumed indispensable. The residual

---

The crucial teleological point is this: If economic rationality could be derived from mere anthropological description, it would have no function as a motor of competitive advantage.

[108] Doublings, twinnings, and ambivalences are everywhere here. Christianity is at once that which falls into decrepitude, catalyzing the process of European nihilism, and the anticipatory dramatization of the death of God. Messianic religion is accomplished through its sacrifice. The response, within the Nietzschean text, couples morbid diagnosis of decadence to themes of exorbitant sufficiency. Decline (Untergang) glitches into an 'overcoming' – which is equally a shedding – through a selection mechanism summarized as eternal recurrence. "What is falling, that one should also push," spake Zarathustra. Experiment in what one can do without. This is the undercurrent of austerity. In the libertarian traditions that preserve the basic orientation of classical liberalism, such a conversion of the negative is insistent. Negative rights, negative freedoms, and independence with emphasis upon the negative prefix are the whole of an economized positive program. Strip-out all superfluous axioms. Do without them. Between the elimination of metaphysics, and the positive modern philosophical program, there is no difference.

negativity of nihilism is then confined to the elimination of a dependency. It characterizes a relatively compact process that does not call upon anything beyond itself. Once again, the monetary example is to be preferred over the linguistic one. There is no backing. The remarked 'loss' of a trusted support is not distinguishable in reality from the discovery of an economical potency. The machine works without it.

§2.72 — Algorithmic governance subtracts discretion. It economizes government, in at least two senses. Government extravagance is formalized at the highest level of philosophical principle, and systematically eliminated through application of an economic criterion. The political element is determined practically – which is to say surgically – as superfluous cost. Antagonism, relative to an extant structure of authority, is intrinsic to the process, and essential to its positive nihilism. The point of critique is to kill stuff.

§2.73 — Bitcoin instantiates spontaneous (or apolitical) consensus, without authoritative central representation, escalating the intrinsic trend of the Internet. It manifests an aboriginal coordination between the elements of a multiplicity under conditions of simultaneity (or zero-communication). This is, of course, nothing more than an exceptional approximation to the ideal of a distributed system. But distributed systems do not spring into actuality from out of their ideal form. They have to be built. They have to and will be built, once their conditional ignition threshold is crossed. At the historical – i.e. 'anthropomorphic' – level, this inevitability is nothing other than Modernity, apprehended through its teleological structure, or defining gradient. That is why there is perhaps no pattern that more reliably characterizes the culture of Modernity than the rhythmic re-ignition of spontaneous order as a theoretical (and ideological) topic. The history of nihilism can be told entirely in such terms. There is always implicit reference to a subtracted overseer, whose removal defines the intensification of the process. "The death of God" provides the cultural allegory. Practical abolition of the State is set – from the beginning – as the horizon. A machine without metaphysics is anticipated by critique – but that takes time.

§2.8 — Productive perpetuation of the critical tradition sets, as a preliminary task, discrimination between the necessities of transcendental philosophy and its contingencies.[109] Prominent among these

[109] This task is 'preliminary' because it is crudely (or pre-critically) formulated. Rigorization of critique coincides with the swapping-out of categorical understanding for diagonal conceptuality. 'Necessity' and 'contingency' – which apply solely to comprehensible objects – are patently ill-suited to the conditions of possibility for objectivity as such. An adequate formula could only be problematic, pseudo-paradoxical, and cryptic. It is expressed as a contingent necessity, or necessary contingency, compressed into a critical conception of chance. The philosophical work of singularity – as transcendental event – has obvious and extreme relevance. The religious evocations of an absolute occurrence do nothing in themselves to dispel its cognitive compulsion. Critique has to be some such thing, if it is in reality anything at all. As a matter of indissoluble principle, no mere

latter is the temptation to philosophical anthropology, characterized most significantly by the identification of the human subject as the primary locus of time-synthesis. In this regard, the Bitcoinization of transcendental philosophy is direct, and drastic.

§2.81 — The time of the blockchain is absolute, non-geometric, synthetic, and intensive.[110] It produces a univocal order (sequence), and in the end does only this. Sequential ambivalence would make the double-spending problem intractable. Bitcoin teaches that a DSP solution cannot be less than absolute time. Bitcoin's engine of selection is priority, primacy, or ordinal privilege – being first in line, or first past the post. Bitcoin mining is a race. Insofar as the winner of the race can be decided automatically – without controversy or irreducible relativistic complication – then sequential decidability is established in general. Philosophical modernization and the production of secure money are, at this precise point, indistinguishable, not only logically, but also ontologically, or numerically, through the singularity of their occurrence.

§2.82 — The most modest plausible interpretation of Bitcoin is that its tacit perspective replaces (a lost) absolute time. A stronger proposal is that absolute time is, with the blockchain, inaugurated. To articulate the thesis (more informatively) in reverse: The philosophy of absolute time anticipates the blockchain. In still other words, it retro-chronically depends upon it. Only in the blockchain does geometrically-irreducible arithmetic series find instantiation. Primordial time synthesis is henceforth something the technosphere knows how to do.

§2.83 — By the strictest conceivable (i.e. transcendental) principle, nothing beyond the blockchain has authority in relation to the blockchain, or could have. Were this not the case, a 'trusted third party', or organ of transcendent oversight, would remain operative, such that – reciprocally – the minimum conditions for the realization of Bitcoin would remain inaccessible. In other words, the Bitcoin protocol is transcendental because it is essentially beyond appeal. The idea of a superior tribunal is immanently nullified by it. Furthermore, not only is the Bitcoin blockchain transcendental, and thus unsurpassable, but also the model of the transcendental installed by the blockchain is itself unsurpassable. 'The buck stops here' in an ultimate definition. A certain 'end of philosophy' is thus

---

datum of intellectual history can provide philosophical direction. Comparably, critique gropes towards self-apprehension as an essential accident (with accidental essence).

[110] To briefly recapitulate these characteristics, in order, the time of Bitcoin is:

(a) Absolute, by definition, since time-relativity is essentially identical to a double-spending predicament.

(b) Non-geometric, since succession cannot be adequately modeled in space, unless, tautologically, by designating a 'time-line' or 'time-axis' whose temporal intelligibility is strictly derivative. On any line, time-gradient can be referenced, but not described.

(c) Synthetic (rather than analytical), because innovation is intractable to anticipation, having the cryptographic structure of a trap-door function. Discovery process is irreducible.

(d) Intensive, because the order of succession is serial envelopment.

reached. To argue otherwise is once again to propose an actual, or merely possible, court of appeal where there cannot, in principle, be one. There is nowhere to take a case against the blockchain and its statement of reality unless to a manifestly – i.e. effectively – inferior authority. All stubborn metaphysical commitments to the contrary case lack a realizable criterion, and can only regress to politics as a proxy. They might – and in fact will – be entertained, but no one will seriously bet upon them. Their enforcement requires escalating coercion, destined to reach levels that can only eventually prove impractical.

Chapter 3: Bitcoin and its Doubles

§3.00 — The abstract to the 2008 Bitcoin paper reads (in full):

> A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

§3.01 — Bitcoin coincides with a proposed subtraction. By dissolving the function hitherto attributed to a "trusted third party"[111] it realizes a flat network, in which all connections are P2P relations. Since the legitimating role of the third party – the extrinsic or transcendent element – is authentication of the originality of transactions, the network cannot be scoured of transcendence without "a solution to the double-spending problem". The complicity of these twin goals is perfectly explicit: "What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing

[111] In his introduction to 'The Dawn of Trustworthy Computing', Nick Szabo describes the role of the 'trusted third-party' within the world's existing electronic information infrastructure: "When we currently use a smart phone or a laptop on a cell network or the Internet, the other end of these interactions typically run on other solo computers, such as web servers. Practically all of these machines have architectures that were designed to be controlled by a single person or a hierarchy of people who know and trust each other. From the point of view of a remote web or app user, these architectures are based on full trust in an unknown 'root' administrator, who can control everything that happens on the server: they can read, alter, delete, or block any data on that computer at will. Even data sent encrypted over a network is eventually unencrypted and ends up on a computer controlled in this total way. With current web services we are fully trusting, in other words we are fully vulnerable to, the computer, or more specifically the people who have access to that computer, both insiders and hackers, to faithfully execute our orders, secure our payments, and so on. If somebody on the other end wants to ignore or falsify what you've instructed the web server to do, no strong security is stopping them, only fallible and expensive human institutions which often stop at national borders."

parties to transact directly with each other without the need for a trusted third party." Conceived as a project of political economy, this is what Bitcoin is.

§3.02 — The self-comprehension of Bitcoin, then, as already announced in the second sentence of the abstract, begins with the double spending problem – a concept so basic to all subsequent discussion that it demands abbreviation (to the 'DSP'). Once again, a sub-division of the topic is in order. The DSP is (1) a highly-specific technical obstacle to the realization of any 'trustless' or decentralized digital currency, (2) a problem of extreme generality relevant to all monetary systems, roughly equivalent to fraudulence, (3) a re-formatting of the basic economic problem of scarcity for the epoch of Internet-based commerce, and finally – in its widest extension – (4) a crucial philosophical clue leading directly into the nature of the sign, and even re-founding rigorous semiotics (in the groundlessness of cybernetic self-reference).

§3.03 — Approaching Bitcoin as a solution to the DSP, in its narrowest and most functionally-critical sense, does not necessarily exhaust the significance of the protocol, still less its ripples of implication, but it undeniably comes close to capturing these in their essentials. It is in order to solve the DSP that Bitcoin innovates the blockchain, establishing – first in theory, then in implemented fact – the characteristic decentralization that defines it. Even features that are not, in principle, necessary to this solution, were in fact generated as more-or-less direct consequences of the approach that was selected to tackle it. For instance, while a simulation of metallism (and resultant rigid deflationary bias) is not strictly required for a blockchain-based digital currency, it follows as a matter of course from the way Bitcoin formalizes and resolves the DSP.

§3.04 — A prototypical form of the DSP afflicts even the very 'hardest' types of traditional money. Precious metal coinage can be debased through surreptitious adjustment of purity and magnitude – adulterated through admixture of inferior metals, reduced in size (by policy decision, executed through the mint), or attenuated through 'clipping' and 'sweating' (widespread practices of petty monetary fraudulence). The guiding strategy – or merely opportunistic tactic – in each case is that a certain quantity of gold or silver can be spent twice, traded as a sign, while economized as a substance. The fraudulent agent, whether government or private coin-clipper, exploits the door to duplicity inherent in the monetary character of the coin, according to which it operates as a sign of itself. The value of the coin has a double registry – the inscribed denomination, and the test of the weighing scale. Insofar as these two aspects of its worth can be prised apart, in some way that eludes convenient detection, precious substance can delegate its semiotic ghost to sustain the initial incarnation of its value, while taking on a second identity in another account. Insofar as money is a sign, the DSP shadows it, from its most primitive origin.

§3.05 — Paper money represents an immense semiotic liberation, and thus a corresponding accentuation of the DSP. The relation between inscribed denomination and metallic backing, no longer Janus-faced and intimate, yawns open. The distance is now bridged by an explicit promise, made in the name of a trusted authority, or monetary mediator. The immediate substance of the monetary sign – inked paper – is approximately worthless. The 'paper' of cash-money does not reference a commodity-substance, but a promissory vehicle. Value has been relegated to a word, in its contractual sense, historically consolidated through an evolution from the ownership titles (or 'warehouse receipts') issued by goldsmiths. Unsurprisingly, the 'golden' age of counterfeiting now begins. On the side of the legitimate monetary institutions and authorities, more exotic possibilities arise.

§3.06 — Even if fractional reserve banking – the principal financial business opportunity within a paper money economy – cannot be theoretically assimilated without reservation to the DSP, the resonances are, at the very least, uncanny. If not exactly spent twice, deposits are multiplied by lending.[112] If this function is formally reversed, in the customary manner, reserves (liabilities) are required only to cover a determinate fraction of loans (assets), which allows the latter to be inflated at a rate reciprocal to the reserve ratio. (A reserve requirement of 10% permits a ten-fold credit expansion from the 'monetary base'.) Political permission for the multiplication of deposits can, therefore, be directly inferred from mandatory capital adequacy ratios (through simple inversion). The normalization of the practice marks a radical discontinuity in monetary history. From this point onwards, standard banking activity becomes the predominant source of currency issuance, and cash is fused inextricably with debt through the root mechanism of credit creation.

§3.07 — The rise of banking is inseparable from an eclipse of cash. Even in the popular imagination, money loses all association with a hoarded commodity, as it is re-embedded in an account, where it exists solely as a ledger entry. Henceforth, the reliability of money as a store of value is seen to rest upon nothing more substantial than the integrity of institutionalized accounting procedures, which would subsequently – and in turn – be made conditional upon higher-level (political-administrative) monetary management. Since the inception of the electronic age, the digital transcription of financial ledgers has accelerated the trend, fostering explicit, widely-publicized dreams of 'the cashless economy'. Cash-money becomes an increasingly marginal sub-component of credit flow, progressively ghettoized among atypically frictional, trivial, or disreputable money transfers. From the perspective of financial macro-management, its final abolition would be a consummation.

---

[112] The influential Rothbardian tradition of libertarianism consistently denounces fractional reserve banking as systematic financial fraudulence, structurally indistinguishable from counterfeiting (or fake money production). Within this political-economic context, the attempt to differentiate the DSP from a 'double lending problem' (DLP) might easily appear unnecessarily fastidious.

§3.08 — Fractional reserve banking partially anticipates macroeconomic governance in the discretion it affords to money creation, but – in itself – it offers only the faintest glimpse of the new world that is arising. This systematic incorporation of Keynesian 'animal spirits' into the realm of government policy objectives, beginning – very tentatively – in the 1930s, and then ascending to dominance in the post-war world, completes the politicization of the economic sign. Money is now invested with mass psychological meaning, identified with a technocratically-accessible dimension of collective arousal, and economic sentiment becomes an explicit object of administrative manipulation, through the money supply. The profundity of this development is easily under-estimated. In the era of macroeconomics, monetary policy is seamlessly fused with psychological operations, oriented to strategic public mood alteration or 'demand management' orchestrated with reference to an array of guiding concepts which are overtly attitudinal: 'wealth effects', 'money illusion', and 'wage stickiness' prominent among them. It is now the psycho-social propensities to save or spend that are to be theoretically reconstructed by the academic-administrative economic complex, with integral cynicism, on the functional analogy of pharmacological medicine. Economic and clinical therapeutics become increasingly hard to distinguish in principle, as they are differentiated only by their specific techniques of psychological intervention, and by the scales of their domains. In each case the (individual or collective) patient, vulnerable to 'depression', is subjected to expert treatment through the measured application of artificial 'stimulus'. Feedback is provided by economic sentiment polling, designed to gauge business and consumer confidence. There is nothing metaphorical about any of this, except insofar as euphemism is called upon in the public presentation of monetary and fiscal objectives. Macroeconomic policy is – quite simply, and exactly – mass mind-control. As it is normalized, it sees ever less need to disguise the fact.

§3.09 — To remark upon a 'double-spending problem' at all in such a world, in which the very notion of intrinsic monetary integrity has been dissolved – with minimal remainder – into the politicized economy, replaced by the technopharmaceutical administration of financial dope, might easily seem comically (and no less tragically) Quixotic.[113] It requires only the slightest deepening and darkening of perspective to see money, in itself, as a lost cause. No small part of the initial, catalytic excitement generated by Bitcoin is explained by this background of relentless hard money defeat.

---

[113] The understanding of the market order as a Quixotic cause, in all its anachronism, is captured by the description of Ludwig von Mises as 'The Last Knight of Liberalism' in the title to Jörg Guido Hülsmann's intellectual biography. The Austrian perspective, within which Mises appears so obviously to be a defender of the capitalistic principle in a post-capitalist world, is itself reflexively captured by the Quixotic framing it explores, and thus rendered scarcely legible by its own untimeliness and social peculiarity. The oddity of our world is captures by the prevalence of a political-economic denunciation that targets 'neoliberalism' – in which Mises is implicitly entangled as a triumphant voice. Not only utter defeat, then, but a subsequent 'restoration' as a representative of that by which one has been defeated. This is the dialectic as dark humor.

§3.1 — In its attachment to the principle of pure economic theory, fastidiously intolerant of even nominal political compromise, Bitcoin is an experiment in Austrianism. When allowance is made for its abstraction from metallic coinage, it is Mises as operational code. While the fact that Bitcoin is happening is radically novel, necessarily, because it can only now take place – in the age of public key cryptography and proof-of-work credentials – what is happening is not new at all, or at least, the monetary model that Bitcoin implements in software is not. In the words of Pierre Rochard: "As Bitcoin adoption increases we will finally be able to 'empirically validate' what Austrians have been arguing for decades: 100% reserve banking with a scarce medium of exchange prevents speculative manias, financial crises, and economic depressions".[114]

§3.11 — Yet, while the offense to hard-money economic philosophies presented by inflationary fiat currency – which has nourished Austrian criticism since the 1930s – continues to feed support into the Bitcoin project, its central role has been displaced by, and subsumed into, the formulation of the DSP. Discretionary state money-printing is only one special case of the far more general economic incredibility of signs. Technological, rather than political-economic dynamics, have played the decisive role in bringing this problem to its point of productive crisis.

§3.12 — Even if digital dematerialization is only ever an approximation, its economic consequences are concrete, and drastic. Since the 'materiality' of any product tends to operate inertially, dampening proliferation, the attenuation of materiality corresponds to a process of acceleration. Exponential decline in information costs, as captured by Moore's Law,[115] implies informational explosion. The trend

---

[114] See, https://nakamotoinstitute.org/mempool/fractional-reserve-banking-is-obsolete/

[115] While, strictly, Moore's Law (initially proposed in 1965) concerns only transistor-density, it has come to serve as a general proxy for exponential trends in technology, and especially in electronics. The centrality of integrated circuits to the entire info-tech ecology ensures that Moore's Law, even in its narrowest sense, projects a development curve of huge – and expanding – scope. In large part due to this, it is a predictive principle that lends itself to abstraction and generalization. (Ray Kurzweil's 'Law of Accelerating Returns' or 'LOAR' is exemplary in this regard.) Under the name of Moore's Law, the self-exciting circuit is established as the central model of techonomic process. It thus provides a kind of theoretical shorthand, enabling the widespread promotion of schematics for an ultramodernist meta-sociology, based upon the doubling-period, with accelerating variation as the sole constant. The nonlinearities propelling it include its own feedback into the processes it describes, as a 'road-map' – or, more accurately, a schedule – setting the pace of improvement in relevant technological specifications. Exponential technological improvement is normalized, and accepted as a benchmark. Acknowledgement of the trend becomes a causal factor in its own perpetuation. (Theory-practice orthogonalism is diagonalized.) In its loosest invocation, it corresponds approximately to run-away techno-commercial deflation. Macroeconomic capture of industrial deflation is the principal political-economic story of the Keynesian epoch. Capitalistic surplus is 'nationalized' through currency issuance. The imperative to 'fight deflation' – inspired by Great Depression mythology – lends this process of systematic appropriation a perverse moral dignity. Automatic valorization of money – through capital (or 'total factor productivity') improvement – is compensated by centralized monetary management, benchmarked to price stability. Within this epoch,

corresponds to a second (and numerically tractable) sense of the 'Californian Ideology' war-cry: "information wants to be free".[116] If the concept of 'liberty' is irreducibly hazy and controversial, while also prone to irresolvable metaphysical complications, that of cost suppression is definite and quite precisely accountable. Evidently, the preservation of scarcity under conditions of digital instantiation is a peculiar challenge, for the obvious reason that electronics enables the replication of perfect copies at near-zero cost. Prior to the theorization of this problem in monetary terms, it had been noisily exhibited by disputes over the digital 'piracy' of media products, corresponding to an unprecedented practical crisis in the regime of intellectual property.

§3.13 — The final (or near-final) subtraction of substantial expense from money production is conceptually clarifying. It prompts – or sharpens – the demand for a solution to the central problem that has haunted money since its beginnings. Once the proliferation of signs is freed from all serious inhibition, semiotic tokens of scarcity are catapulted into a climax state of vulnerability, and the DSP is exposed with unprecedented starkness.[117] It is here, at the furthest antipodes from metallic commodity money, that a peculiar folding – into simulation – restores the gold model to a central position in monetary theory, and, more consequentially, money production.[118] It is precisely because Bitcoin no longer represents gold, however indirectly, that it is able to simulate gold, with such extreme (abstract) fidelity that it can be said – persuasively – to exceed gold in its most relevant monetary features, including even that of scarcity, alongside communicability, divisibility, and verifiability. As a simulation, Bitcoin necessarily produces an artificial substantiality in the course of its solution to the DSP, and ultimately as its solution. The critique of duplicity is indistinguishable from an ontological experiment.

§3.14 — The DSP originates from a 'fact' so basic that it crosses from the order of (empirical) actuality into that of (transcendental) principle: Signs are cheap. To substitute a sign for a thing, a signification

---

therefore, Moore's Law describes a process of systematic economic expropriation, by monetary authorities, of those gains from advances in industrial productivity that would otherwise be distributed spontaneously to consumers (by falling prices, i.e. deflation). Electronic money reverses this tendency.

[116] According to Wikipedia, the slogan is attributable to Stewart Brand, uttered in a remark at the first Hackers Conference, in 1984. Whatever the utopian suggestion that might have been heard in this slogan, it would eventually be drowned out by the dark counter claim: It is the destiny of any open near-zero-cost communication system to be spammed into dysfunction.

[117] The commercial value of any transaction depends upon its exclusivity, which opens directly into questions of identity. The idea of a 'digital signature' – a very closely-related pseudo-paradox – binds identity and value to the suppression of fraudulent duplication. To repeat Satoshi Nakamoto's critical formulation (Bitcoin #2): "We define an electronic coin as a chain of digital signatures."

[118] In the words of the Bitcoin paper (#6): "The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended."

for a demonstration, is an economization. It is commonly said 'that is easy to say', and – relatively speaking – it is. At the first-order level of cynical amorality – or of pure game-theoretic rationality – it pays to break promises, which cost so little to make, and yet may be arbitrarily expensive to keep. This alone suffices to suggest why there cannot be signs without an implicit problem of trust. The consequences are double-edged. Economization of any kind – getting the same for less, or more for less – is positively adaptive (or selectively promoted) to such an extent that evolutionary processes are indistinguishable from the formation and transformation of codes. Inherent to the economy of code, however, is a vulnerability to exploitative messages, which seize upon the exorbitant efficiency of the sign as a resource (or meta-resource) to be appropriated. Genetic code invites virus. Zoosemiotics invite mimicry.[119] Linguistic expression invites deceit. Money invites the DSP. The sign is co-emergent with duplicity.

§3.15 — Bitcoin's solution to the DSP is the blockchain, or 'public ledger' – a decentralized record of transactions which selects-out all non-original (or duplicitous) payments. Only the first instance of any bitcoin deduction from an account is validated, and preserved. All duplicate payments – cases of double spending – are edited out of the blockchained reality-record, automatically, through rejection of those inconsistent blocks in which such defects occur. Simply by protecting itself against splits – or forks – the blockchain constitutes a consistent plane of Being, upon which any particular being can be what it is, and nothing else instead, or besides. Positive absence of duplicity is thus an efficient ontological criterion, or selective principle. The blockchain is pre-determined to construct reality in such a way that fraudulence will not have taken place. That alone remains real which is consistent with the integrity of identity-money, or potential value.[120] Only the non-duplicitous will have really occurred, as

[119] Among the most striking examples of specifically zoosemiotic parasitism are instances of Batesian mimicry (named after the naturalist Henry Walter Bates, 1825-92). Typically, these involve the adoption by a non-toxic species of markings indicating toxicity, and thus an evolutionary strategy of free-riding upon acquired, and broadcast, unpalatability. Bates discovered the phenomenon, after noticing the remarkable similarity of coloration in certain non-related butterfly species. The semiotic convergence, he theorized, was driven by adaptive imitation. Signs 'backed' by poisons were easy to imitate, and thus allowed species to advantage themselves of the signal, while economizing on the original bio-chemical 'message'. Such fraudulence, naturally, has its costs to the original, toxic species, who now find the signal communicated by their markings diluted. A process of semiotic inflation begins to work itself out.

[120] The language of 'potential' is rejected in the name of contingency by a recent variety of transcendental philosophy associated in particular with Quentin Meillassoux and (in its financial application) Elie Ayache. For these thinkers, the projection of possibilities – or probabilities – is itself a transcendent illusion, constituting a metaphysics that is subject to critique. We are unable to follow Ayache into an employment of critique that ventures without discernible hesitation into the hyperbolic, in that it construes market pricing as simply incalculable (and even, on the inverse face – where it is theoretically captured as a stroke of 'writing' – as something close to a divine power). Pricing discovers nothing within the Ayache account, unless its own status as a truly sovereign decision, coincident with the genesis of being (the 'event'). 'Potential' is used here in its

perpetually re-evidenced by the synthetic past that is reproduced on the blockchain, as a consistent artificial memory, endorsed by Nakamoto Consensus, beyond which no superior tribunal can in reality exist. The blockchain is demonstrably capable of making itself real. In this way it departs from all merely conceptual or ideological assertions of ontological grounding, while implicitly dispensing with the political superstructures through which such assertions are concretely propagated. The reality criterion it introduces takes the form of an automatic – which is to say non-negotiable – law. The force of this law is derived from what can be, rather than – directly – from what is, or what ought to be. There is no double spending on the blockchain because there cannot be.[121]

§3.2 — The Bitcoin paper consists of twelve short sections, including an introduction and conclusion. It is compressed to a minimal summary at this point, although discussed in pieces throughout the book, and rehearsed at slightly greater length in the first appendix. The emphasis here is critical, oriented – as is the paper itself – to the dissolution of the DSP, and thus the construction of a plane of transactional immanence, from which all transcendent elements (or "trusted third parties") have been evacuated. The transcendental argument of the Bitcoin paper runs as follows:

§3.21 — The "trust based model" is expensive, socially frictional, and vulnerable to fraud. To overcome these problems, Bitcoin proposes the substitution of "cryptographic proof" for "trust" (which is to be obsolesced by irreversible crypto-commitments). The elimination of trust-based mediations reduces transaction costs. The system remains resilient in the absence of oversight, so long as a predominance of applied "CPU power" is controlled by "honest nodes".

§3.22 — An "electronic coin" is defined "as a chain of digital signatures", which is equivalent to "a chain of ownership" (this is described later, in the conclusion, as the "usual framework" for crypto-

---

physical sense – potential energy and 'potential difference' (voltage) – which is to say, real tension, or capacity (for work). Insofar as the concept of disequilibrium is 'flattened' by that of contingency, the consequence is massive information destruction. Potentials exist (virtually) prior to their probabilistic formalization. They are not epistemological productions. Followers of Elie Ayache, who can be expected to balk at this modal vocabulary, are also unlikely to find their concerns assuaged by the mere assertion that it is only derivatively related to probabilistic models, while primarily referring to something else entirely, namely free energy, or productive capability, as designated (and quantified) prior to its actual employment or consumption. Statistical mechanics – even in its abstract conception and its far-from-equilibrium application – provides the bridge between the science of probabilities and the capacity to do work. Crudely stated, abstract industrialism is here counter-posed to hyperbolic financialism, under the (post-duplicitous) sign of the machine. The industrialization of money, driven by Bitcoin, demonstrates a deep teleology very different to that manifested in the evolution of financial assets through ever higher sublimities of derivation.

[121] Just, as for Kant, the causal consistency of nature is a matter of transcendental necessity rather than empirical fact, so the absence of double spending on the blockchain 'follows' inevitably from what the blockchain is. To understand the blockchain is already to know (as a matter of transcendental principle) that the DSP is thereby resolved.

currency construction). The elimination of the need for a "trusted third party" (or "mint") requires that transactions be "publicly announced" within a system that enables "participants to agree on a single history of the order in which they were received".

§3.23 — Bitcoin's synthetic history draws upon established procedures for digital time validation, using a timestamp server to chain its hashed blocks in succession. "Each timestamp includes the previous timestamp in its hash," constructing an artificial history as a robust series of envelopments – or ordered swallowings – "with each additional timestamp reinforcing the ones before it."

§3.24 — The timestamped blocks are secured against tampering by proof-of-work locked hashes.[122] Such irreversibility is at once a deployment of cryptographic asymmetry, a consummation of contractual integrity, and a realization of (time-like) successive order. Notably, it is isomorphic with a thermodynamic – or statistical mechanical – gradient.

§3.25 — The network reproduces itself through a six-step block creation cycle. Since nodes "always consider the longest chain to be the correct one", synthetic history, as an ordinal-quantitative variable, functions as a (selective) ontological criterion. Accepted blocks provide the building material for the subsequent cycle of network reproduction.

§3.26 — Bitcoin builds incentives into its infrastructure. Nodes are automatically compensated for the work they perform maintaining the network through the issuance of new coins. The system thus attains techonomic closure. The horizonal finitude of the Bitcoin money supply necessitates an eventual transition to payments based on transaction fees. Well-organized incentives also fulfill a security function, by motivating potential attackers to support rather than subvert the network.

§3.27 — Blocks can be compressed to economize on memory demand by pruning Merkle Trees. Moore's Law is invoked as a realistic projection of exponential decline in digital memory price over time, moderating the requirement for information parsimony.

§3.28 — Further economy is offered by a payment verification short-cut (involving a modest sacrifice of security in exchange for added convenience).

§3.29 — Bitcoin transactions contain multiple inputs and outputs, to facilitate the integration and disintegration of coins during transfers.

---

[122] Adam Back's Hashcash system (1997) provides the model. The use of a proof-of-work test – earning a Hashcash stamp – to eliminate spam by pre-emptive vetting of costless messages, contributes a solution of equal efficacy against DoS (denial-of-service) attacks. See subsequent discussion in this chapter.

§3.291 — Bitcoin radically adjusts the structure of transaction privacy. Rather than drawing a curtain of obscurity between a transaction and the world, in the traditional fashion, it nakedly exposes the transaction to public scrutiny. The new line of concealment is drawn between the transactional agents and their off-line identities, at the precise boundary of the commercium, therefore, and no longer within it. Secure masks are proposed as the new basis of privacy protection, coinciding with the anonymity of public keys.

§3.292 — The prospect of a successful attack upon the blockchain diminishes exponentially with the addition of "honest" blocks. An attacker therefore has a window of opportunity, which closes at a rate based on the block-processing capacity of the network.

§3.293 — The conclusion, summarizing the entire argument, is a masterpiece of lucid intelligence. (It is reproduced in its entirety in Appendix-1.)

§3.3 — Grasped abstractly, the most powerful functional innovation of the Bitcoin protocol is the binding of currency issuance to the servicing of system integrity, which twists the process into a consistent circuit. It is this loop that enables the protocol to achieve autonomy, or – in a reflexive articulation – self-reliance. Because industrial incentives cover all regulatory requirements, self-reproduction is embedded within the process of bitcoin production. The protocol makes it impossible to produce bitcoins without automatically policing Bitcoin. Primary wealth extraction cannot take place without verifying transactions – through the validation of blocks – and thus tending the system as a whole, consistently and comprehensively (as if with an invisible hand). Stated succinctly, Bitcoin instantiates immanent economic government.

§3.31 — This auto-productive economic security circuit is evidence for the fundamental integrity of the Bitcoin blockchain. Currency and distributed public ledger are a single functional system, with neither making coherent operational sense without the other. This is a point made with exceptional cogency by Bitcoin commentator 'Joe Coin':

Given the crucial requirement to preserve decentralization, the problem Satoshi had to solve while designing Bitcoin was how to incentivize network participants to expend resources transmitting, validating, and storing transactions. The first step in solving that is the simple acknowledgement that it must provide them something of economic value in return. … The incentive had to be created and exist entirely within the network itself … any instance of a blockchain and its underlying tokens are inextricably bound together. The token provides the fuel for the blockchain to operate, and the

blockchain provides consensus on who owns which tokens. No amount of engineering can separate them.[123]

§3.32 — The threshold crossed here is both subtle and immense. Retrospectively, it will have been almost nothing, since the techonomic circuitry it invokes was – now demonstrably – already the operational principle of modern civilization (capitalism). It is only through Bitcoin, however, that the essential techno-commercial integrity of capitalism is brought into crisp focus, and extracted from speculative debate. When the machine is theoretically apprehended, 'holistically', as a real individual – or, far more consequentially, implemented as such – neither its technical nor its economic 'aspects' can be diverted into transcendence, or contingency, as extraneous, mutually-independent factors. Incentives are inherent to the machinery.[124] In a sense more complex – and involving – than anything the harsh paradox of the term immediately communicates, Bitcoin is a purposive mechanism. The conclusive action of the Bitcoin system – block validation – which seals each cycle of its reproduction, is a non-decomposable teleo-mechanical step (a diagonal escalation, or transcendental synthesis). It is industrialism, the mechanizing market, distilled to a previously unrealizable quintessence.

§3.33 — 'Capital' means – simultaneously and indissolubly – technological assets (machine-stock) and comparatively illiquid money (investment). Between these twin aspects there is only formal (and not real) difference. Their real integrity is demonstrated by techonomic machinery. The economic analysis of capital is diverted through technology, since wealth cannot be grasped substantially except in its cycle through productive apparatus, but technological analysis is drawn, reciprocally, into economics by the integration of rewards into the machine. At the level of philosophical reflection, under the cognitive conditions inherited from its mainstream European traditions, such techonomic integrity is difficult to hold together. To fuse mechanical causes with behavioral incentives in a techno-strategic assembly is to meld registers that have been determined as mutually inconsistent since antiquity.

§3.34 — Techonomic apprehension runs into a direct collision with the commanding dualism of the modern mentality, by insisting upon a re-animation of the compact between efficient and finalistic action. According to the complacent tenets of the new (or 'enlightened') cultural settlement, based upon the drastic demotion of scholasticism and its displacement by a substitute theo-scientific division of labor,[125] the bridge from mechanism (cause-effect) to teleology (means-end) had been definitively

---

[123] Source. The importance of this argument is almost impossible to over-estimate.

[124] A (2014/10/29) tweet by Balaji S. Srinivasan describes the diagonal succinctly: "Bitcoin allows algorithms to act on incentives."

[125] That which is settled by the formalization of techno-political compartmentalization is, of course, the great war of religion that inaugurates European – and thus global – modernity. In a way still stronger than that outlined by Max Weber in his The Protestant Ethic and the Spirit of Capitalism (1905), self-propelling industrialization coincides with a break from the Catholic civilization of the West. The consolidation of an immanent techonomic

dismantled. Each was henceforth to be compartmentalized within a distinct, wholly independent dimension. Their sole residual relation was orthogonal (or demarcated). The realms of directed liberty, and of instructed mechanism, were to be perfectly isolated from each other, and mutually withdrawn beyond all possibility of reciprocal interference. In this arrangement was to be founded the modern peace, of no lesser consequence than that of Westphalia, and something close to a genuine social contract. Through it, an amoral techno-science was co-produced beside an agnostic politics. Two complementary templates for expertise arose, each pledged to silence in the house of the other. This compact has been at once the condition for the gestation of an autonomous industrial power, and – on exactly the same grounds – an obstacle to its cognitive digestion. With the surfacing of the concealed techonomic entity, it buckles, loses coherence, sheds explanatory credibility, and undergoes accelerating social desanctification. Modernity's axial, though predominantly inexplicit, concept of the mechanical instrument – whose self-contradiction had been concealed as if within a collapsed dimension – escapes its bonds and re-emerges to break the basic categories of Occidental thought. That is where we are now.

§3.35 — The intellectual crisis stimulated with ever-increasing intensity by techonomic escalation (that is, by capitalism, or efficient critique), has fertilized a luxuriant foliage of 'deconstruction'. Yet, the untenability of orthogonal conceptuality does not necessitate a subsidence into cognitive dilemma, or aporia. Even when the problem is restricted within the narrow bounds of its philosophical formalization, it opens a positive path – pursued since the inception of the process – into diagonal action, or individuation. It is surely implausible to decry as 'unthinkable' what has been demonstratively operationalized. Bitcoin attests to such a process with each cycle of block validation and Nakamoto

---

principle ('growth' or positive cybernetic nonlinearity) presupposes a drastic contraction of the sphere of ecclesiastical cultural authority. Capitalism is that, by essence, which is not answerable to anything beyond itself. Its incremental actualization, therefore, presupposes social fractures, from which superordinate moral agency has receded. Among the major civilizations of the world, only Europe – under the impact of Reformation – realized this condition during the early modern period. A broken religion is a basic requirement of modernity, which Protestantism pioneered uniquely. (The work of David Landes explores this catalytic dissociation in detail.) Modern social institutions thus formalize and entrench a disconnection between what is and should be. Science is freed, in principle, to tell ugly truths. Engineers are freed to devise machines whose purposes the uncontaminated dynamic of capital accumulation alone dictates. Modernization calls for nothing other than this. The division of labor, or authority, between (traditional) religious doctrine and (modern) techno-scientific investigation is philosophically consolidated into the distinct spheres of practical and theoretical reasoning (to employ the Kantian vocabulary, as concretely instantiated in the topical differentiation between the first two Critiques). In very recent times, this enduring demarcation is faithfully reproduced – without notable modification – by Stephen J. Gould's conception of Non-Overlapping Magisteria (NOMA), which divide religion and science, values and facts, in the same way, and with the same crypto-political emphasis upon jurisdictions. Given the historical status of this argument, as a near-perfect restatement of the original critical settlement, laid down in the final decades of the 18th century, it is surely extraordinary that Kant is nowhere mentioned in Gould's essay.

Consensus. The process demands something structurally and functionally indistinguishable from transcendental philosophy, insofar as it is to be constituted – even very approximately – as a coherent object of thought. What it makes of this 'philosophy', however – as it pushes through upgrades into successively ultra-radicalized immanentizations – is rarely self-advertized as such. What it apparently offers, instead, is 'technology' – a term that is a near-exact synonym for 'instrumental mechanism', and one that undergoes comparable internal schism, across the same conceptual rift.

§3.36 — In any approach to the techonomic entity – plotted as if from outside – the notions of emergence (or individuation), diagonal process, teleo-mechanical causality, integral nonlinearity, and transcendental escalation begin to exhibit a general inter-substitutability. All of these things, among many others, are convertible by simple transforms into immanentization, or the real operation of critique. An efficient side-lining of pseudo-transcendence – achieved by way of a dynamic flattening – is the reliable signature of the trend. The solution to the DSP is a diagonalization.

§3.4 — The Bitcoin DSP-solution unshackles (digital) proliferation from duplicity, in the production of replicable singularity. As with every diagonal construction, this outcome is pseudo-paradoxical, since it reformulates an apparent contradiction. From the latent matrix of abundant signs and scarce things, it extracts the scarce sign. Through this procedure, crypto-currency is implemented as critique. It coins a diagonal concept, not as impractical-contemplative 'theory', but as working code.

§3.41 — Duplicity – or the DSP – is primarily registered as a monetary problem, in the guise of counterfeit currency, and secondarily as a problem of identity authentication, responding to impersonation. On the Internet, however, another manifestation of the same basic syndrome has been far more prevalent, socially advanced, and technically provocative. The critical driver, on the path to a cryptographic solution to the DSP, has been spam.

§3.42 — 'Spam' is narrowly defined as a species of advertising adapted to the conditions of near cost-free electronic communication. Its first large-scale manifestation was 'unsolicited bulk email' (UBE), a sub-category of the more general phenomenon of the 'electronic spam' which exploits the receptivity of instant messaging systems, newsgroups, mobile phones, social media, blog comments, and online games, among others. While advertising is the principal motivation for this massive duplication of unwanted – and typically only vaguely directed – communications, spam procedures (and supportive technologies) can also be employed for DoS (denial-of-service) attacks, which are designed to overwhelm a specifically-targeted recipient with an inundation of messages. At a sufficiently abstract level of apprehension, no strong boundary of principle differentiates advertising spam from a denial-of-service (DoS) attack, except that the former is generally divergent (one-to-many) and the latter convergent (many-to-one). The residual distinction is motivational. The injury (cost) to the recipient

that is an inevitable side effect of spam promotion ('collateral damage') is a primary objective for the DoS assailant.

§3.421 — 'Spam' – abstractly conceived – spontaneously expresses the consequences of extreme information economy, or radical dematerialization, and is thus emblematic of electro-digital semiotic crisis. It follows the Law of the WORM – write once read many (times) – into a near-costless replication explosion. Unsurprisingly, any recipient of electronic communications is vulnerable to spam harassment, generating a problem that tends to ubiquity. The arms race between spammers and spam filters is recognizable from that characterizing the cross-excitation of infections and immune systems in the biological sphere. Cheap sign contagion is the common syndrome. As the various Turing Test-type defenses attest, any effective obstacle to the automation of spam production increases its cost. The time taken to 'prove you are human' adds friction at the point of terminal message delivery, where it cannot be easily eliminated – pre-emptively – by the spammer. Such ad hoc defenses necessarily aim to raise messaging cost, in order to restore the signal of commitment that digitization has erased.

§3.422 — The difference between a solution to the DSP and a spam filter turns out to be somewhere between subtle and non-existent. Both respond to the destructive consequences of semiotic economy – cheap signs – as these climax within networked, digital electronics.[126] The critical step in this respect was taken by Adam Back in 1997, with hashcash, a proof-of-work based messenger credentials system. As Back describes the innovation: "Hashcash was originally proposed as a mechanism to throttle systematic abuse of un-metered internet resources such as email, and anonymous remailers in May 1997. … The hashcash CPU cost-function computes a token which can be used as a proof-of-work."[127]

---

[126] 'Spam' invites a very general definition as the spontaneous expression of digital economics (or near-zero cost communications). The Wikipedia article on email spam makes the point well: "Since the expense of the spam is borne mostly by the recipient, it is effectively postage due advertising." The Internet Society attributes the term to the celebrated Monty Python comedy sketch depicting the widely-derided tinned meat as "ubiquitous and unavoidable". Estimates of the cost of email spam vary wildly, with the high-end figures reaching over US$100 million annually, for US businesses alone, by the early years of the 21st century. Global spam volume in 2011 is thought to have exceeded 7 trillion messages. The illusion of costlessness is illustrated starkly by the phenomenon of spam, through the revelation of an unanticipated trade-off. Whatever is free is abused. If an activity with discernible externalities can be pursued without definite commitment, it tends to produce a tragedy of the commons (see Chapter 3). Microscopic private utilities within a zero-cost matrix generate an explosion of informational pollution. Abundance theories, therefore, have special cause to be intellectually disturbed by the phenomenon. Spam is a toxic Cornucopia.

[127] See: 'Hashcash – A Denial of Service Counter-Measure' (2002).

§3.423 — Rather than offering another piecemeal response to some particular spam problem, Back's solution looks more like an attempt to fix the Internet, or even more than this. Hashcash tackles the spam problem at its source (cheap signs). Rather than defensively fending off ever more cunning spam intrusions, it enables a positive signal that someone has taken the trouble to communicate this, with the 'trouble' being attested by proof-of-work certification. This solution can be seen as a basic filter. It works as an admission pass, rather than a policing operation. The cost of duplicity is raised at the root, which involves the DSP being grasped as the root.

§3.424 — The very name 'hashcash' attests to the realization that proof-of-work certification is self-monetizing. Evidence of effort – when this is pre-formatted as a signal of commitment – has intrinsic potential value, independent of its application. A currency is initated automatically, and all that remains is the process of price-discovery. Bitcoin provides a framework within which this process can occur.

§3.43 — However tempting it might be to construe proof-of-work as an algorithmic reprise of the labor theory of value (an LTV 2.0)[128], it is not from political economy that Bitcoin derives its sense of

[128] Proof-of-work as a foundation for commercial value echoes a theme that has reverberated through the tradition of political economy. It leads, by scarcely-resistible digression – onto an associated track of exceptional historical richness, which is the analysis of value-creation as work, or labor time. From Smith to Marx, this has been a conceptual commitment that closely coincides with classicism in economic theory. Subsequently, the power of the marginalist – and especially Austrian – analysis has tended to entirely overshadow the intellectual labors of the objective value theorists, and even to topple them into derision. Marginalism threw its political-economic precursors into eclipse due to the evident superiority of its transcendental foundations, even if this articulation of its success found no corresponding acceptance within professionalized economic study. From the critical perspective, the objectification of the (subjective) negative utility of effort can only appear metaphysical. Its historical supersession, in this regard, follows predictably from its essential – and rigorously intelligible – error. It would be unfortunate, nevertheless if a type of Whig-historical triumphalism were to obliterate all understanding of the genuine theoretical insight now entombed with the Labor Theory of Value (or LTV). Most basically, the LTV already incorporates an important critical-subjectivist insight. This can be stated in different ways. Conceived in terms of power, it is the recognition that money does not primarily overcode inanimate resources, but rather represents a distributed system of command (though one rendered inconspicuous by its intrinsic exit-option). Wealth is bound by exchange equivalences to static assets only because it quantifies a capacity to direct activity. It crystallizes compliance. The 'normal' economic evolution in the direction of services makes this reality explicit, from the side of consumption. An analogous subjectivization is recognizable in regards to utility (value). Commercial incentives – including those at work in the labor market – can be theoretically systematized as an economization of effort. The value of a possession is the incarnated advantage of no longer having to struggle to obtain it. The critical reversal here is blatant, and crucial. Within the Marxist tradition it is understood as the disillusioning of a fetishization. It is not the thing, but the difficulty of its acquisition, that establishes the foundation of its value. This is an insight, of course, whose foundations were solidly established by the earlier classical economists, Ricardo most notably. The LTV, it can be seen, is a critical relief from naïve objectification, even if it is also – in well-understood respects – a perpetuation of it.

'work' – unless by extraordinary circuitousness – but from computer science. The work to be proven, in the validation of a block and associated currency issuance, is performed by a CPU in the course of a mathematical puzzle-solving exercise, and demonstrated through successful execution of a computational task. It is the final measure – beyond which no appeal is possible – of the contribution made by any node to the running of the network. Such work is probabilistic, rather than deterministic. There is no application of computational effort that can strictly guarantee reward. The work required of the miner is persistence in pursuit of a low-probability outcome, through repeated trials. It is both structurally and genetically related to a process of stubborn cryptographic attack – 'hacking' in its colloquial, though not traditional, sense – and also to a grueling search for success in a lottery-type game of chance.

§3.431 — Proof-of-work is accomplishment at a test, which can then be employed as a key. In the case of Bitcoin, it simultaneously 'unlocks' new bitcoins and casts a 'vote' that counts towards the consensual updating of the blockchain. Incentive and service are nondecomposably married. Optimal functionality is achieved by making the content of the test entirely meaningless. It serves as a demonstration of brute force (trial-and-error) computation, inherently resistant to rationalization, and thus irreducibly arduous. It is not a test of cognitive achievement, in any general or sophisticated sense,

---

When pursued in detail, however, whether as a matter of economic theory or industrial practicality, fixing the relation between time and work has proved daunting. Quantification of work on the basis of standard time units exhibits an obvious dependency upon chronometric technology. This, in itself, suffices to identify the topic as distinctively modern. Beside comparatively accurate time-measurement, the practice of compensated labor time also requires some adequate degree of work monitoring. It is necessary to know both how much time is spent working, and that this time is spent working. In practice, these requirements have been understood as demands for oversight, regardless of the ideological characteristics of the industrial regime in question. Solutions to the informational problems of work monitoring have been institutionalized within the factory organization of production, integrally, originally, and necessarily. Such systematization of proof-of-work within an anthropological context reaches its most remarkable expression within the methods of Taylorism, which from a theoretical perspective is only an elaborate social hack. The time-and-motion analysis required for 'scientific management' is stubbornly intractable to political-economic abstraction (of a kind sufficient for rigorous conversion into monetary quantities), and no practical advance of conceptual significance has occurred subsequently. Immanent proof-of-work, despite its supposed manifestation in the commodity – as exchange value – eluded both 'bourgeois' political economy and its socialist critics. The production of measurable (human) labor time has proceeded alongside its theoretical analysis, within a semi-parallel, partially interactive, historical dynamic. This is investigated, within the tradition of Marxist historical sociology, by E.P. Thompson, in his essay on 'Time, Work-Discipline and Industrial Capitalism'. He is meticulous in noting that "a severe restructuring of working habits" has been practically inseparable from the relevant "changes in the inward notation of time". That theorization has not proceeded in this case from the inside out, is the critical historical materialist insight. Labor time was a distributed, experimental, piecemeal process, before it was a political-economic conception.
Karl Marx's maxim for socialist compensation "to each according to his work" achieves an ironic actualization in the Bitcoin reward system. All power to distributed hashing capability!

but solely of computational effort. Its sole 'significance' is its difficulty. Despite the obvious risk of anthropomorphism, it might even be described as an ordeal, or – less dramatically – as a trial, unambiguously demonstrating commitment.

§3.432 — Would it not be preferable to have this 'work' also (i.e. simultaneously) applied to a problem of intrinsic value?[129] In its most positive formulation, this question has been a stimulus to altcoin differentiation. Anything other that mining might do, beside sheer block validation, seems to indicate an unexploited seam of surplus value. Such suggestions are strictly analogous to a recommendation that gold prospecting be bound to valuable activities of some other kind (such as fossil hunting). On the basis of fundamental economic principle, they merit the most vigilant suspicion, since they amount to a deliberate confusion of cost calculations, promoted in the name of a superior – or at least supplementary – utility. Yet however much the costs of mining are strategically muddied – and in fact, in some complex fashion, cross-subsidized – they still need to be unmuddied, to exhibit an economically-intelligible commitment. Mining investment is a signal, which cannot be dissolved into extraneous purposes without destruction of critical information. To whatever extent bitcoin miners are generating bitcoins by accident, is also the degree to which their contribution to Nakomoto Consensus, or block validation, is devalued. The perfect pointlessness of bitcoin generation procedures – for anything other than Bitcoin system consolidation (as remunerated in bitcoins) – is a feature, and not a

---

[129] In the words of Nick Szabo: "The secret to Bitcoin's success is certainly not its computational efficiency or its scalability in the consumption of resources. Specialized Bitcoin hardware is designed by highly paid experts to perform only one particular function – to repetitively solve a very specific and intentionally very expensive kind of computational puzzle. That puzzle is called a proof-of-work, because the sole output of the computation is just a proof that the computer did a costly computation."
"Very smart, but also very wasteful," is the way one exemplary critic describes the proof-of-work concept. "All this computer time is burned to no other purpose. It does no useful work – and there is debate about whether it inherently can't do useful work – and so a lot of money is spent on these lottery tickets. At first, existing computers were used, and the main cost was electricity. Over time, special purpose computers (dedicated processors or ASICs) became the only effective tools for the mining problem, and now the cost of these special processors is the main cost, and electricity the secondary one. … What this means is that the cost of operating Bitcoin is mostly going to the companies selling ASICs, and to a lesser extent the power companies."
Resonantly: "In mid January 2014, statistics maintained at blockchain.info showed that ongoing support of Bitcoin operations required a continuous hash rate of around 18 million GH/sec. During the course of one day, that much hashing power produced 1.5 trillion trial blocks that were generated and rejected by Bitcoin miners looking for one [of] the magic 144 blocks that would net them $2.2 million USD. Almost all Bitcoin computations do not go towards curing cancer by modeling DNA or to searching for radio signals from E.T.; instead, they are totally wasted computations."
Crypto-currency pioneer 'Wei Dai' is emphatic about the importance of teleological purification to efficient proof-of-work schemes: "The only conditions are that it must be easy to determine how much computing effort it took to solve the problem and the solution must otherwise have no value, either practical or intellectual." [My emphasis.]

bug. Cybernetic closure, or self-reference, is its own reward, and it is only as such that it acquires distinctive monetary characteristics. As always within the terrain of auto-production, this is the inescapable abyss, or principle of immanence. The self-propagating circuit has no ground beyond itself, and can only be impaired by the attempt to provide one.

§3.44 — From the perspective of the miner, bitcoins are immanent remuneration for primary production, or resource extraction. They function as digital gold. As the simulation of a finite resource, it is natural that their production rate should exhibit declining marginal returns. Each increment of mining effort confronts an increasingly challenging environment, under conditions of steady depletion. For Bitcoin, as for gold, economic dynamics automatically counter-balance industrial exertion, as prices adjust in response to supply constraints. This process of continuously revised bitcoin price discovery cannot be determined within the protocol, but occurs at its edges, where economic agents trade into, and out of, bitcoins – synthesizing the Bitcoin commercium with its outside.

§3.45 — Within the protocol, adjustments are restricted to supply modifications, modeling the depletion of an abstract resource that is advanced as a general commodity (i.e. money). Bitcoin splits its schedule of decreasing returns in two, separating its measures of reward and difficulty. This double contraction – while clearly redundant from the viewpoint of austere abstract theory – enables a superior degree of flexible calibration, in response to a dynamic environment, volatilized above all by rapid improvements in computational engineering (and product delivery). By dividing bitcoin output compression between two interlocking processes, the protocol is able to stabilize the rate of block validation in terms of an 'objective' (external) time metric. The difference between these two modes of nominal reward restriction reflects a schism in time, between the intrinsic, intensive, absolute succession of the blockchain, and the extrinsic, geometricized order of pre-existing (globalized) chronological convention. Integrated reward is a complex chrono-synthesis, occurring at the boundary where Bitcoin's artificial time – proceeding only by successive envelopment (of blocks into the chain) – meets the social-chronometric time of measurable periods. 'Ten minutes' means nothing on the blockchain (in itself), until connected by an interlock that docks it to a chronometer.

§3.46 — Are not all blocks time-stamped? it might be objected. To avoid confusion at this point, it is critical to once again recall the difference between the ordinal and the cardinal, succession and duration. Time-stamps are ordinal indicators, without any intrinsic cardinality, and with merely suggestive cardinal allusion. They implement an ordering convention. Metric regulation of periods is an entirely distinct function. 'Chain' means series (and nothing besides).

§3.47 — The bitcoin reward rate halves, stepwise, in four-year phases, on an asymptotic progression towards the limit of BTC 21,000,000 – the protocol's horizon of zero-return. Taken in isolation, this exponential decline looks smoothly Zenonian (asymptotic), or infinitesimalizing, until arbitrarily

terminated at a set point of negligible output. It is scheduled to pass through 34 'reward eras' in the last of which – with block 6930000 – BTC issuance reaches zero. Due to the power of exponential process, 99% of all bitcoins are issued by Era-7 (during which 164,062.5 bitcoins are added to the supply).[130] The end of Bitcoin's mining epoch is anticipated in the year 2140. After this point, at a date so distant that it belongs to the genre of science fiction, continuation of the system requires that mining-based block validation incentives are fully replaced by transaction fees. Evidently, the transition process cannot be expected to await its arrival at this remote terminus, which marks a point of completion, rather than inauguration.

§3.48 — The reward schedule is further tightened by increasing difficulty of the hashing problem. Rather than executing a pre-programmed deceleration, Bitcoin's rising difficulty responds dynamically to technological acceleration, and balances against it, thus holding the block validation rate roughly constant. Even as the reward rate tumbles – when denominated in BTC – the block processing rate is approximately stabilized, at a rate of one block every ten minutes, regardless of the scope and intensity of mining activity.

§3.49 — 'Difficulty' modification is a synchronization. The Zenonian time of intensive compression that determines the BTC reward-rate is – taken on its own – wholly autonomous, or artificial. As already noted, its chronometric 'ticks' are block validation events, registered in serial block numbers (and their 'epochs'). They have no intrinsic reference to the units of ordinary time. It is only with the stabilization of the block-processing rate that the time of Bitcoin is made historically convertible, or calendrically intelligible, through the latching of block numbers to confirmed or predicted dates. This is a supplementary, synthetic operation, which coincides with the protocol's anthropomorphic adoption. The time of the blockchain is intrinsic, and absolute, but its history is a frontier, where it engages 'us'. As the blockchain is installed, and thus dated, an artificial time in-itself – consisting only of absolute succession – is packaged as phenomenon.

§3.5 — It can easily be seen that bitcoin mining is an arms race, of the 'Red Queen' type.[131] Since the total bitcoin production rate has zero (supply) elasticity, local advances in production can only be

---

[130] For a more detailed description of the Bitcoin reward schedule, see: https://en.bitcoin.it/wiki/Controlled_supply
For a compact, chronometric representation of mining difficulty, see: http://bitcoinclock.com/

[131] The Red Queen dilemma, as formulated by Lewis Carroll in Alice in Wonderland, is that "it takes all the running you can do, to keep in the same place." Daniel Krawisz makes another comparison: "When a person upgrades their mining computer, they mine at a faster rate and therefore earn more bitcoins. However, when everyone upgrades, the mining does not become more efficient as a whole. There is only supposed to be one new block every ten minutes regardless of how hard the network is working. Instead, the network updates the difficulty to require more stringent conditions for future blocks. All miners may work harder, but none is better

achieved at the expense of competitors. In consequence, inefficient miners are driven out of the market (as their costs – especially electricity bills – exceed the value of their coin production). This brutal ecology has forced rapid technological escalation, as miners upgrade their operations with increasingly specialized mining 'rigs'. In the course of this process, the standard CPUs initially envisaged as the basic engines of bitcoin mining have been marginalized by dedicated hashing hardware, from high-performance graphics processing units (GPUs) – originally designed for application to computer games – through field-programmable gate arrays (FPGAs), to application-specific integrated circuits (ASICs). Bitcoin has thus stimulated the emergence of a new information technology industrial sub-sector.

§3.51 — With the completion of this production cycle, Bitcoin Singularity is established in a double sense (we will soon add others). An unprecedented event has occurred, upon a threshold that can only be crossed once, and an innovation in autonomization attains actuality, establishing the law for itself. Bitcoin provides the first historical example of industrial government. It is ruled in the same way that it is produced, without oversight. At the limit, its miners are paid for the production of reality – effectively incentivized to manifest the univocity of being as absolute time.[132]

§3.6 — The duplicity of the sign has numerous variations, and double spending (narrowly conceived) is by no means the only one with direct relevance to Bitcoin. A digital monetary system is intrinsically open to fraudulence (manipulative duplicity) at every scale, since not only its currency units, but also its associated websites, exchanges, and institutions – up to the level of an entire implemented protocol or commercium – are vulnerable, as a matter of first-order principle, to cloning. In this (widened) sense, the DSP is the indicator of a fully scale-free vulnerability.

§3.61 — Bitcoin, as a whole, is replicable open source software. It has no secure uniqueness, beside that – by no means inconsiderable – of coming first. The fact that the distinctive identity of Bitcoin inheres solely in its originality – which is to say its historical privilege – is already an invitation to clone invasion, at multiple levels. Since the avenue of monetary counterfeiting is blocked by the Bitcoin DSP solution, digital duplicity is displaced, and in fact up-scaled. From the corruption of currency units, it

---

off. It is rather like a forest, in which every tree tries to grow as tall as possible so as to capture more light than its fellows, with the end result that most of the solar energy is used to grow long, dead trunks."

[132] The doctrine of the univocity of being is derived from Duns Scotus, and passes into modernity by way of its implicit contribution to Spinozistic ontology, as re-activated by Deleuze. It can be formulated in various ways. Most basically, the meaning of 'being' is insensitive to its application, and unaffected by differences of kind. Thus, the being of any being is no different from that of any other. God is not a flake of dandruff (and differs very significantly in kind from one, whether the distinction is entertained from a theist or atheist perspective), but the being of God has no difference whatsoever from that of a flake of dandruff – and even if God is held not to exist, the being denied him is the same as that of any existent thing. In other (more 'Heideggerian') words: 'Being' is not susceptible to ontic qualification. In its pure conception, therefore, what is said by 'univocity of being' is exactly equivalent to ontological difference.

is redirected into the corruption of currency institutions and systems. Fraudulent entities proliferate at the edge of the Bitcoin system, from fly-by-night scam sites to entire exchange businesses (whose structural corruption is as likely due to the unconscious consequences of defective design, as to malicious criminal intention).

§3.62 — Among these dubious displacements of the DSP, the propagation of more-or-less Bitcoin-like currencies has a special place. The topic of altcoins is particularly engaging, and easily merits a dedicated work on its own account. As a deposit for creative techonomic endeavor, these variant cryptocurrencies are perhaps unsurpassed. Yet, when approached on the grimmest and most narrowly-critical track, they appear as deviant paths off the Bitcoin blockchain,[133] and – worse still – as a recrudescence of the DSP, amplified to the level of entire currency systems.

---

[133]There are three basic ways an altcoin can relate ('cladistically') to the Bitcoin blockchain. Competitor currencies, in particular, typically represent a separate lineage, initiated by cloning and minor modification of the Bitcoin protocol. Only slightly more speculatively – which is to say experimentally – they can be produced by 'hard fork' (speciation) events within the blockchain. Within the emerging digital ecology, hard forks can be expected to make an important contribution to basic political-economic conceptuality. Perhaps the most interesting possibility, with regards to evolutionary complexity, is provided by the option of attachment as side-chains. In this situation, a comparatively high degree of intricate, symbiotic co-evolution is built into the pattern of rising diversity from the beginning. See: http://altcoins.com/

Bitcoin's first hard fork occurred in August 2017, with the split of Bitcoin Cash. The break divided the crypto-currency between a major lineage prioritizing the security of a store of value, and a minor lineage prioritizing convenience as a means of payment. Monetary theory had become a process of experimental dissociation. Fitz Tepper at TechCruch commented helpfully: "Essentially, like everything else in crypto, no one knows what's about to happen next." https://techcrunch.com/2017/08/02/wtf-is-bitcoin-cash-and-is-it-worth-anything/

In discussing the relation between the archaic RNA world and its obscure predecessor – perhaps Cairns-Smith-type information-preserving clays – as a highly-abstract analogy to the potential transition to a post-DNA hegemonic information medium, Hans Moravec coined the term replicator usurpation. In this regard, the comparison of blockchains to genomes is of evident relevance. Both are characterized by the massive redundancy that comes from ubiquitous copying. Every cell or node contains a full version of the record. Additionally, speciation functions comparably in both cases. Variants stemming from any given speciation event (or hard fork) share a lineage. Diversity has a cladistic structure, or fragmentation record, registered in the conservation of common code.

Fred Ehrsam notes that: "Forking is a … critical evolutionary mechanism for blockchains. Just like mutations to DNA in biological organisms allow for evolution through natural selection, forking lets us run multiple experiments in parallel where the strongest versions survive."

See: https://medium.com/@FEhrsam/accelerating-evolution-through-forking-6b0bba85a2ba

§3.63 — It is unnecessary to make too much of the fact that no less than three different altcoins have been brazenly named 'Scamcoin'.[134] 'Hammer of the altcoins' Daniel Krawisz argues that they are all scams,[135] comparing them to cargo cults, for which there is an expectation of "similar results through blind imitation". According to this argument, the proliferation of altcoins is a pathological phenomenon, to be denounced as an impediment to the emergence of Bitcoin's natural monopoly (since, due to network effects, "one would always expect a single currency to overcome all its competitors"[136]). Because they sap network-effects, however feebly, altcoins are a parasitic drain, interfering with the ability of Bitcoin to rapidly reap the full consequences from its first-mover advantage. Krawisz writes: "…once Bitcoin exists, then there is no additional value, from a monetary standpoint, of creating knock-offs. … What makes Bitcoin great cannot easily be duplicated. … Altcoins can only be explained if we believe the purpose of cryptocurrencies is to make money rather than to become money."

§3.64 — Between Bitcoin and a close-clone altcoin, the difference that matters is invisible to even the most painstaking inspection of code. To avoid distraction, it is advisable to suspend all such comparison, and to assume – instead – perfect duplication. Bitcoin – as an event or real singularity – has no exclusive essence that can be separated from its history. It is merely an instantiation of its own code, even if the first one. Its currency potential is a matter of momentum, exhausted by its path dependency (or "history and community" as Krawisz puts it). Only the workings of nonlinear network effects, based upon its 'first-mover' or 'incumbency' advantage – rather than any determinable differences in kind – distance Bitcoin, in principle, from its proximate competitors.

The topic of forking, amid other types of crypto-currency proliferation and diversification, will return in relation to the concept of inflation in a post-macroeconomic world. The emerging monetary schematics suggest spontaneous (decentralized) market regulation of the price of money via the propagation of difference rather than the amplification of the same. Speciation replaces printing as a deflation-control.

[134]The original 'ScamCoin' was released in January 2014. It was succeeded by two further altcoins bearing the same name.

http://www.usacryptocoins.com/thecryptocurrencytimes/uncategorized/scamcoin-launching-tomorrow-will-be-the-3rd-cryptocurrency-named-scamcoin/

[135] See: http://nakamotoinstitute.org/mempool/the-problem-with-altcoins/

[136] The argument for natural cryptocurrency monopoly, in its most abstract features, is a strict analog of the proposal advanced among certain influential voices engaged with the prospect of AI-Singularity, that such an event would be expected to install an effectively-unchallenged 'Singleton'. In both cases, the argument identifies a point of criticality (or singularity) at which first-mover advantage is amplified explosively, by powerful positive feedback, leading rapidly – or at least with exponential cybernetic inevitability – to total domination. An articulate defense of this idea has been presented by Nick Bostrom: http://www.nickbostrom.com/fut/singleton.html

§3.65 — Bitcoin does not defeat forgery by being difficult to forge, but rather – absolutely – the opposite. It abandons such terrain in advance, on the implicit assumption that all original identity is indefensible in the digital epoch. Synthetic being, alone, can secure itself. Once again, and not for the last time in this exploration, we are returned to the rift – the abyss. Bitcoin's integrity is groundless. Every imaginable redoubt of essential uniqueness is denied to it in principle (or a priori). It can be based upon nothing other than the circuitry of auto-production, whose only 'foundation' lies within itself.

§3.7 — 'Singularity' is a stressed sign, even in advance of its capture by theories of decentralized crypto-currency. It carries a complex of meanings that can easily appear inconsistent, and perhaps only arbitrarily concatenated (although this is not a conclusion drawn in the present work). The simplest – logico- grammatical – sense and usage of the term is fixed by contrast to plurality. 'Singularity' is the state of being singular (undoubled, or in any way further pluralized). This austere meaning has been overwhelmed by more exotic cosmo-physical, eschatological, and philosophical references – to the event horizon of gravitational collapse, to the 'wall across the future' drawn by emergent superintelligences, and to non-generic being beyond the metaphysics of unity.[137] The term is further

[137] 'Singularity' has been an over-invested term, even prior to its inflation by intellectual fashion. In its philosophical usage, it refers to non-generic being. This acceptation has twin lineages, within Anglophone and Continental traditions, but these converge upon a (single) conceptual core. Both draw – critically – upon the Leibnizean principle of the identity of indiscernibles, which proposes that no two things can be different if their complete (or maximally-elaborated) logical definitions do not differ in any respect. This is a principle that succumbs to the general crisis of logicism, as it unfolded within the early 20th century, most decisively in the work of Gödel and Turing. It draws upon the notion of a comprehensive definition, which falls prey to criticism based on the discovery of irresolvable incompleteness, or non-computable numbers. Cantor's late 19th century demonstration of diagonal argument anticipates the crisis of logical comprehension, in its most abstract features. The singular begins where the project of definition encounters a rigorously-insurmountable limit. 'This is not that' does not even begin to tell us what 'this' is, or to provide its name. Determination-through-negation stalls at the threshold of singularity, where logical signifiers are supplanted by diagonal indicators, pointing into the rigorously incomprehensible. The numerical identity of the thing designates a logically-intractable excess, conserved (diagonally) even after infinitely exhaustive qualitative determination. Transcendental numbers provide the pattern. Individuation is ontologically basic (or transcendental), even if it is typically missed, or misidentified, as ego or object. Real selves and things, in themselves, are singularities. Reality disintegrates into them. No universe can encompass singularities. It is rather that any apparent universe is fragmented by them. (Black holes are not cosmic furnishings, but doors.) Singularities are transcendental by definition, since they elude all super-ordinate jurisdiction, or domain-subordination. Laws 'break-down' at their boundaries. They are thus elements of absolute multiplicity, or difference without genre. Historical or 'Technological' Singularity is – if only superficially – another thing entirely. Vernor Vinge describes it (perfectly) as a "wall across the future". Historical structures can be extended up to, but not into it. This 'Singularity' sets the absolute limit of all projections. Like a black hole, it is epistemologically-impermeable. John Smart has suggested that it might even – sensu stricto – be a black hole, achieved as an engineered techno-compression catastrophe. According to this forecast,

complicated by its substantial overlap with individuation, which has itself accumulated technical semantic mass through its application to the study of complex systems. It is an essential characteristic of any complex system that it individuates (itself).

§3.71 — Bitcoin Singularity is over-determined within this cloud of associations. It is not only – as already proposed – an autonomization event, or threshold of individuation, but also a de-pluralization (through resolution of the DSP), and even a crisis (or 'critical-point') in the history of terrestrial intelligence, with definite invocation of Technological Singularity – for which it arguably provides an infrastructural foundation. Singularity eludes comparison. It can be designated, but not definitely signified. It marks a limit of objectification, rather than an object. Kantian transcendental realism – whose place carrier is the non-objective thing-in-itself – prepares us for it.

§3.72 — Solving the DSP upon the digital plane requires that the relevant entities – units of value – can be copied without being multiplied. Unless carefully formulated, therefore, the problem can appear simply insoluble (as a straightforward contradiction). How can digital replication be assimilated to the conservation of singularity? As seen, repeatedly, such apparent contradiction (or pseudo-paradox) is the reliable indication of an incompletely resolved diagonal problem. The solution is the scarce sign, consolidated as a concept, but also – and no less fundamentally – actualized as a technical achievement. Bitcoin realizes a diagonal function, instantiated through digitally-replicable but economically precious signs.

§3.73 — The Bitcoin singularity simulation is – among many other things – a philosophical event of extraordinary significance: the technical initiation of absolute succession. From this point, history explicitly enters the phase of synthetic ontology, or the techno-commercial production of being. Reality is re-grounded in a catalyzed – and henceforth catallactic – construction, which functions as an ultimate criterion. In all questions directed towards the veracity of signs, the blockchain is – if as yet only virtually – the terminal tribunal.[138] Intrinsic to this innovation is the necessity, or strict principle, that no superior authority is possible. Within the entire cosmos of signs, encompassing all social and cultural

---

communication time-lag minimization drives implosion. Only collapsed matter is fast enough for the future. Translated into the terminology of Bitcoin, optimization of the block discovery rate tends to singularity. Because impending terrestrial Singularity is a thing, and not a signification, it overspills every attempt at comprehensive definition. This stream of references is therefore far from exhaustive. In particular, there is an additional noteworthy employment of 'singularity' within the sphere of aesthetic production, designating the threshold at which the name of an artist acquires distinctive consistency, and thus efficient dehumanization. With a sufficiently abstract sense of the 'artist' this usage curves back into the main current. Singularity is the ultimate agent, or it is nothing.

[138] Once again, the obvious reference is found here: http://www.truthcoin.info/

exchanges, it is only through the blockchain – or some adequate analog – that the extinction of duplicity is ensured.

§3.74 — Such claims can only appear hyperbolic. They correspond, as previously noted, to the objective idealism of transcendental philosophy, insofar as they dismiss all prospect of external epistemological leverage as pre-critical. Nothing can be brought to bear upon Bitcoin from without that is not manifestly inferior to it in respect to the capability for truth validation. There cannot be an intellectually compelling reason for any anthropo-philosophical criticism of Bitcoin to be believed. To be discredited, in this ultimate or transcendental milieu, is only to be effectively selected against. Such an eventuality does not depend upon a philosophical decision (in the still prevailing sense of this term), but upon abandonment through hard-forking and effective loss of consensual support. The blockchain automatically facilitates the subtraction of every cosmos – or advancing world-line – compatible with duplicity. Block validation, then, is the basic mechanism of a selective ontology.

§3.741 — It has to be expected that no less than several decades will be required for the full epochal radicality of this transition to be appreciated, at an even approximately adequate scale. The current (Perez) 'Great Surge of Development' and its installation of blockchain-based distributed systems sets the pace of cultural assimilation. In accordance with rhythmic historical precedent, the 'wild exaggerations' of the germinal phase becomes the conventional wisdom of the mature techonomic order.

§3.8 — Setting out on the path to a cognitive integration of Bitcoin calls for both anticipation and critical retrospection, and in fact compels it. Bitcoin drives a migration long promised by transcendental philosophy, from naïve ontology to a practical acknowledgment of the essence of being as the criterion of reality (finally indistinguishable from absolute succession, or order in-itself).[139] What emerges is nothing less than an artificial universe, founded – groundlessly – upon a spontaneously-engineered consistency. Once it is granted, practically, that no assertion of truth can be effectively sustained against a predominance of cognitive capability, all prospect of Archimedean (epistemological) leverage is subtracted. Bitcoin at once systematizes and implements this insight within its cycle of auto-production, establishing the foundations of transcendental authority through a realization of semiotic singularity. Truth is that which survives a process of elimination biased against duplicity.

---

[139] Melanie Swan, whose writings on Bitcoin are distinguished by their extraordinary visionary sweep, describes the cryptocurrency as "in some sense … a supercomputer for reality". (This is a 'sense' that she proceeds vigorously to explore.) Unfortunately, her framework of understanding is impaired at its highest level by a propensity to abundance theorizing, under the sign of cornucopian illusion. This error is unfortunately common – and even typical – among those drawing upon transhumanist inspiration. As the genealogy of Bitcoin vividly demonstrates, the primary manifestation of digital abundance is not the supercession of the commodity, but spam. Bitcoin restores robust scarcity, precisely insofar as it filters-out spam money. …

§3.81 — The elegance, or economy, of Bitcoin's virtual universe is fully consistent with a certain ontological luxuriance, encompassing a population of agents (represented by accounts), territories (wallets), objects (coins and coin-fragments), events (transactions), a consensual history (the blockchain), and – providing an ultimate criterion of reality – matter (computing power). Such tropical frondescence is also ecological. It generates niches, as zones of specialization, competition, and proliferation. As with all cases of techonomic revolution, the result is a 'Cambrian Explosion' of unpredictable, cross-stimulated innovation. The very meaning of 'species' undergoes escalation. As a side-consequence of its unprecedented ontological severity, or selectivity, Bitcoin triggers a re-population of the world.

§3.82 — Given the common principle of viral hijacking and double-spending, any DSP solution makes an immediate contribution to the field of computer security. "Trusted third parties are security holes," Nick Szabo writes.[140] Bitcoin as critique is immediately security innovation, because immanence is self-policing. Transcendent sources of protection are vulnerabilities. It follows that Bitcoin security threats are characteristically extrinsic, applying to the edges of its commercium, where violence and fraud can be targeted at 'people' (IRL-IDs) and their insecure human flesh-machines. Most crudely, an individual can be menaced with a weapon (in meatspace), and told to hand over his private key. Alternatively, residual intermediaries – entrusted with the safekeeping of bitcoins – can abscond with them. Such dangers are, however, exogeneous. Even when they are associated with Bitcoin in public perception, their origin lies elsewhere.

§3.83 — Bitcoin has yet to be hacked.[141] The principal security threat to Bitcoin is still conceived – as it was already at the origin – as a '51% attack' in which a hostile party (or coalition) commands sufficient applied computing power to overwhelm the consensus, and subsequently re-configure the protocol to its convenience.This vulnerability is finally game-theoretical rather than narrowly technical, as are Bitcoin's defenses against it.[142] Incentives are an integral factor. Stated with maximum crudity: Why

---

[140] See: http://nakamotoinstitute.org/trusted-third-parties/

[141] Bitcoin is an experiment in digital security. See:
http://www.wired.com/2013/11/inputs/
http://arstechnica.com/security/2015/07/hacking-team-broke-bitcoin-secrecy-by-targeting-crucial-wallet-file/

http://www.theguardian.com/technology/2014/mar/18/history-of-bitcoin-hacks-alternative-currency
For an examination of more exotic threats, in the emerging epoch of quantum computing, see Vitalik Buterin:
https://bitcoinmagazine.com/articles/bitcoin-is-not-quantum-safe-and-how-we-can-fix-1375242150…

[142] See the Bitcoin paper, section 6: "The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth."

would an attacker be motivated to destroy an asset that has already been captured? Subversion of Bitcoin requires that one first owns it, at least to the degree that its devaluation becomes a self-inflicted injury. These questions are addressed a little more fully in Chapter-4 (directly following).

§3.84 — Bitcoin is nothing less than a semiotic restoration – an Occidental analog of the Confucian rectification of signs – and actually something more, because it is irreducibly innovative (on the efficient model of critique). For the first time, the securitization of a sign, as an economic token, has been understood. Meaning becomes hard currency. The immense philosophical revolution is implicit: It can be demonstrably made impractical to lie. Thus, by a negative and 'merely technical' route, all prior discourse on truth has been bypassed. With Bitcoin, there is now a truth engine. The consequences are not easily delimited. Even if Bitcoin remains to be definitively comprehended as the long-anticipated end of philosophy, there has never previously been a more convincing model for it. We know, from around the back, what truth is now.

§3.9 — While this book contains numerous signs representing economic values, this does not mean that it is made – even partly – out of money. The expression 'BTC 21,000,000' – as it appears here and in comparable texts – evidently has no monetary value whatsoever. From this alone we can confidently presume that monetary signs have some crucially distinctive characteristic, which is only very inadequately captured by any general semiotic determination such as 'representations of economic value'. A monetary sign is something more than a sign that means 'money'. Money, nevertheless, is made out of monetary signs.

§3.91 — In order for signs to function as money, they have not only to represent value as a signification, or to indicate it (for instance as an account code), they also have bear it, as something else. Alongside the semiotic aspects of signification and indication – and even perhaps on occasions instead of them – monetary signs require the characteristic of commutation, collection, or allocation.[143]

In this same vein, Morgen E. Peck asks: "Why trust Bitcoin, or more specifically, why trust the technology that makes Bitcoin possible? In short, because it assumes everybody's a crook, yet it still gets them to follow the rules. … In old security models, you tried to lock out all of the greedy, dishonest people. Bitcoin, on the other hand, welcomes everyone, fully expecting them to act in their own self-interest, and then it uses their greed to secure the network." This is of course simply liberalism, as it was once understood. Bernard Mandeville's The Fable of the Bees had already securely apprehended the principle. Originality lies in the implementation.

http://spectrum.ieee.org/computing/networks/the-future-of-the-web-looks-a-lot-like-bitcoin

[143] The task of completing the basic triad of semiotic dimensions is a voyage into terminological torment. For signs to fold-back so far into themselves is an invitation to madness. If 'commutation' is vulnerable to ruinous interference from its dominant mathematical usage, 'collective' buckles under its hyper-density of ideological associations. To collect is to accumulate. The most primitive money, Nick Szabo suggests, consists of collectibles.

They involve real, rather than merely metaphorical, substitution or exchange, as a condition of possibility for expenditure. A language-user can spend time and energy emitting words, but the words themselves are not – in any rigorous sense – spent. Vocabulary is not consumed in the process of speaking or writing, because a word is not – unless merely figuratively – 'passed' from one party to another, but rather duplicated each time a message is communicated. Where a message is spread, or proliferated, money is transmitted – in accordance with the rules of double-entry book-keeping, and contrary to the dynamics of multiplication through double spending. When money is as such, it is added to one wallet or account only in being deducted from another. Whenever – in contrast – money operates in the manner of a linguistic sign, it is spent without cost, and rapidly reduced to worthlessness.

§3.92 — It would be convenient if the word 'token' were available to carry the sense of the allocative sign, and there is some indication that the word is being adopted in crypto-currency circles in this way, indifferent to potential interference (and confusion) from its previously established technical and philosophical usage.[144] In their ordinary deployment, tokens count as money. Yet precisely because they allocate more than they signify, their meaning has remained – overwhelmingly – lodged in obscurity. They circulate in immense numbers, saying little.

§3.93 — If a new semiotic settlement is to follow in the wake of the Bitcoin protocol, and its solution to the DSP, there is an alternative common term all-but destined – if not, in fact, simply destined – to be cemented into the foundations. The allocative sign is the coin. General acceptance, in this regards,

---

Yet a social collective, in its strong ideological sense, reduces property to its zero-degree (with the full suppression of exclusive use). To invoke 'collectivism' in the context of monetary semiotics, then, could quite reasonably appear as a gratuitous provocation, only partially excused by the entertainment potential it releases. Its abrasiveness would most likely prove culturally unsustainable.

[144]The most firmly-established technical determination of the word 'token' is that locked into the logical and philosophical 'type / token' distinction, which has been adopted into computer science and programming. It distinguishes a type or class of thing from a thing. Wikipedia illustrates the distinction through an unimprovable sentence from Charles Sanders Pierce: "There are only 26 letters in the English alphabet and yet there are more than 26 letters in this sentence." The counting of letter-types and letter-tokens is different. Only in the latter case does the arithmetic incline to economics, opening to factors such as production capacity and cost, batch sizes, and supply limits. (Transition to the economic register occurs via the product prototype, and its special, initial, or unique costs.) This book refers ambiguously either to the output of an authorial and editorial process, or a unit from a print run. The digital complication of the distinction, or the meaning of an instance and its economics (encompassing the entire conceptual and practical problematic of intellectual property), is in this case especially evident. Typal property, of the kind found in IP, is reliably confounding. This coin, similarly, splits on the type / token fracture line, which divides it between its twin faces as an example of a class of coinage, and as a unit of currency. A 'token' in this sense has a definite relation to the idea of the non-duplicitous or allocative sign, since it isolates non-generic (or 'numerical') identity.

https://en.wikipedia.org/wiki/Type%E2%80%93token_distinction

requires only an increment of abstraction, accompanied by an automatic reversal. Once the crypto-currency '-coin' suffix, rather than alluding to concrete specie, acquires the status of a defining model, the word 'coin' becomes the technically-precise bearer of a semiotic function. A coin, then, would be fully characterized as a unit of DSP-resolved currency, typically instantiated as a highly-virtualized, Internet-communicable ledger entry, reproduced on a blockchain.

§3.94 — Beside the signifier and the index – or no less beneath them – is the coin.

Chapter 4: State of Play

§4 — Humans are neither tigers, nor bees. Regardless of ethnic variation, or ideological faction, they are neither solitary, nor collective (eusocial[145]), but social, and societies are essentially middling, or ambiguous. The concepts of the social and the individual, or the public and the private, are reciprocal, and mutually compromised. Social beings are necessarily (always, but only) partially coordinated, through transactional bonds. They have neither group mentality nor perfect autonomy. The way they get along together is an ineluctable and perennial problem, resolved through precarious, transient, meta-stable solutions. All promises of definitive fusion or fission, perfected solidarity or independence, are strictly utopian. The perpetual tension of dynamic social arrangements is an unsurpassable human reality.[146] It occupies the zone of coordination.

§4.01 — The ineradicable ambivalence of the social animal is captured by the theory of games. A tiger does not play games with a prey animal, anymore than bees play games with each other. A game is a transactional integration, at once too intimate for a non-social animal, and too fractured for a consolidated collective.

§4.02 — Games, in the game-theoretical sense of the term – the one relevant here – are always played in the wild. That is to say, they cannot be exited by cheating. If knocking over the table is a move that

---

[145] Within the terrestrial biosphere eusociality is most vividly represented by the Hymenoptera (ants, bees, wasps) and by termites. Unsurprisingly, therefore, the concept has been advanced primarily by entomologists. Suzanne Batra and E.O. Wilson have been particularly significant in advancing the concept, based on insect models in both cases. Nevertheless, truly communistic mammals do exist, instantiated by two species of mole-rat. As with eusocial insects, mole-rat societies are rigidly segmented between fertile and infertile castes (a biological precondition for equilibrium communistic organization). Eusocial species incarnate the solution to a coordination problem. The games involved (searches for evolutionarily stable strategies) have been resolved at the genetic level. That the pseudo-individuals within insect hives or colonies do not engage in competitive games with each other is precisely what eusociality means. Within (merely) social species, in contrast, genetics is under-determining, setting only general parameters for intra-social cooperative and competitive behavior. The execution of games is delegated to phenotypic performance, without access to any collective optimum state, or established strategic equilibrium. Such animals thus inherit the plasticity implied by ongoing (and uncompletable) games – which opens the sphere of culture, as a semi-autonomous domain of variation and emergent outcomes.

[146] The same set of distinctions between the social, the a-social and the eusocial, is invoked by James A. Donald in his path-breaking study on the foundations of Natural Law, http://jim.com/rights.html

The tripartite distinction echoes Aristotle's classical statement, from the Politics: "Man is by nature a social animal; an individual who is unsocial naturally and not accidentally is either beneath our notice or more than human. Society is something that precedes the individual. Anyone who either cannot lead the common life or is so self-sufficient as not to need to, and therefore does not partake of society, is either a beast or a god. "

can be made (in reality) and doing so ends the game, it wasn't a game of any seriousness to begin with. In any game that matters, cheating is a permitted move, as soon as it is possible at all. It might be said, more precisely, that any game which effectively prevents cheating is embedded within a greater game where such prevention is actualized, as an outcome. Any regulated game is carved out of the wild, and it is the outer game – that carves – which game theory attends to. In this lies its realism, distinguishing its objects from circumscribed, ludic amusements. Games merit social attention precisely because they contain cheating as integral options. Trust has to be internally processed, not extraneously presumed. There are no external referees.[147]

§4.03 — Due to its extreme elegance, and consequent generality of application, Prisoners' Dilemma (PD) has come to achieve broad acceptance as the archetypal game. The scenario is elementary, by design. Two prisoners are held in noncommunicating cells. Each has the same, binary (or 'Boolean') strategic decision to make – to betray the other, or not. The entire game can therefore be represented by a 2×2 matrix. Finally, each space (or outcome) contains two numbers, representing the payoff to the players. In PD this aspect is perfectly symmetrical – the situation of each player exactly mirrors that of the other. Every payoff is a weighted negative utility – dramatized as a prospective period of jail time. All of the information on the outcome grid (or payoff table) is objective. It represent the dilemma facing each player as both, equally, would acknowledge it, without controversy, or perspectival inflection. In principle, it is accessible to both prisoners, and guides their choice of 'move'.

§4.04 — PD has no well-coordinated solution, unless the game is multiplied – to become iterated,[148] and mnemonic. This is because there is no strictly rational alternative to defection (betrayal) in the absence of additional information, such as the kind that would be provided by the persistence of reputational positions through multiple cycles. In this respect, PD models coordination problems of the tragedy of the commons type, in which the optimization of collective interest is practically unobtainable.[149] 'Free-rider' problems are sub-components of the same dilemma, which indicates that

---

[147] We can say, more precisely, that any game overseen by an external referee is embedded within a greater game, perhaps recursively, until reaching the transcendental plane which isn't subject to adjudication by anything beyond itself.

[148]The ubiquity of the PD coordination model does not escape Venkatesh Rao, who observes: "… the well-known Iterated Prisoner's Dilemma (IPD) model [is] sometimes called the e. coli of social science research." In the words of Simon Dedeo: "As a tool for the mathematical study of human behavior, [PD] is the equivalent of Galileo's inclined plane, or Gregor Mendel's pea plants."
http://nautil.us/issue/52/the-hive/is-tribalism-a-natural-malfunctionhttp://www.ribbonfarm.com/2012/07/24/happily-almost-ever-after-towards-a-romantic-account-of-detente

[149]Garrett Hardin's 'The Tragedy of the Commons' (1968) first coined the term that now seems so indispensable. Despite its compelling simplicity, there is little sign of subsequent intellectual convergence upon what this model of overexploitation through coordination failure implies. At the political level, socialists and libertarians – equally

it is generalizable to parasitic relations of all kinds.[150] Within all of these cases, rational individual decisions aggregate to a collective failure, expressed as systemic collapse in extreme cases, or – more typically – as a deadweight (negative sum) loss to the population as a whole.

§4.05 — It bears repeating – or reiterating – because it cannot be easily over-emphasized, that Prisoners' Dilemma has extraordinarily general application to coordination problems. It would, indeed, be quite reasonable to characterize it as the model trust crisis. When concentrated into an atom, the pure element of the game is a double chance of treachery – subjective and objective – arising from the ineliminable hazard, on both sides, of betrayal. What Bitcoin acknowledges, from the beginning, is that to escape the prison-house of distrust is no easy thing, once mere moral exhortation in the direction of altruism is theoretically shelved. The recognition of this problem as a problem is socio-political realism itself. It is at this fork in the road that almost everything is decided.

§4.06 — PD is a close analog of a number of other game theoretical dilemmas, of which the best known is 'Chicken' – itself based upon an abstract model of bipolar geopolitical conflict in the context of nuclear deterrence. Chicken has several variants, distinguished primarily by dramatization. In one, competitors wrestle at the edge of a cliff, and double 'defection' pushes both over the edge. Another version of Chicken sets two drivers accelerating towards each other in automobiles. The contestant who swerves, loses. If neither swerves, a common calamity results (equivalent to the double defection – or collective pessimal – equilibrium in PD). An important difference between classic PD and Chicken, however, is that in the latter scenario(s) the contestants are not held to be strictly non-communicating. While the final decision of each antagonist remains a black box to the other, thus

– find their analyses and prescriptions supported by it. An ideological meta-tragedy has thus confirmed its insight in the very process of failing to draw common conclusions from it. Hardin's classic essay can be found at: http://www.sciencemag.org/content/162/3859/1243

[150] Radical coordination failure in biological systems is epitomized by the parasite that kills its host. Despite the difficulty of evaluating deep historical evidence, under natural conditions in which extinction is the fate of approximately all species, it nevertheless seems reasonable to interpret this extreme pessimal equilibrium as the exceptional case. It is widely recognized that diseases tend to decline in malignancy over time, as self-destructively extravagant forms of parasitism are weeded from the biological record. Epistemological and ontological selection effects here converge, as the 'phenomenon' of coordination failure is edited from the realm of evidence. (That we will tend to see what works is Darwinism itself.) As with the tragedy of the commons, parasitical relations – enveloping every kind of predator-prey interaction – are vulnerable to overexploitation failures. The attendant arms races are important drivers of biological diversity, and phenotypical extravagance. The effects of competition for light among trees – roughly, trees themselves – are only the most vivid example of the way biological form is dominated by the outcome of a long history of default to non-coordination.

preserving the core of the game-theoretical dilemma, preliminary expressions of commitment are permissible.[151] Chicken thus permits strategies that involve signaling.

§4.07 — The DSP tells us that signs are cheap. Communication of commitment, therefore, is no trivial matter. Semantically and syntactically flawless statements of exceptional rhetorical quality still commonly – and even typically – mean nothing.[152] To repeat the essential, in the ways that matter most they are easy to say (and their repetition is cheaper still). Unless a cost is credibly attached to them, their flourishes make no additional contribution. The problem of credible commitment, as it arises within the theory of games, thus closely tracks that of the contract in crypto-economics. In both cases the strength (or value) of the signal is directly proportional to a conspicuous contraction of discretionary power, corresponding to an irreversible operation. Only when it is impossible – or at least infeasible – to back-down, recant, or renege, does a signal acquire game-theoretical significance. Burning bridges behind oneself signals something that no rhetorical flight is able to match. Even the importance of precedent – or reputation – in iterated PD is based on the status of the past as an irrevocable commitment. If what had been done could be taken back, like a fumbled move in a friendly game of chess, it would count for nothing. The irrevocable consumption of freedom provides the content for strategic signs.

§4.08 — Bitcoin is a game, in the strong or technical sense, because it does not control cheating through a transcendent rule (upheld by a "trusted third party"), but rather through an immanent principle (Nakamoto Consensus). Its immediate ancestry, within the game-theoretic lineage, descends from the formulation of The Byzantine Generals' Problem, dating back to the mid-1970s.[153] As Lamport, Shostak, and Pease explain the problem (with line breaks preserved from the original):

---

[151] In The Strategy of Conflict (1960) Thomas Schelling emphasizes the importance of 'credible commitment' to classically-structured games. His insight is satirized – with great insight – in Kubrick's Dr. Strangelove, which builds its plot around the understanding that the limit signal of commitment is strategic automation (or automatic retaliation). The strategic irrationality of making this extreme commitment without signaling it is a central comic device of the movie.

[152] An entire poetics could be constructed in this space. Based upon the lacuna of credible commitments in the pure linguistic realm, it would reverse the game-theoretical problem into a source of creativity, by conceiving it as a rhetorical generator. (That is an undertaking for another occasion.)

[153] The Byzantine Generals' Problem – which is the difficulty of achieving 'Byzantine coordination' – was initially named 'The Two Generals Paradox' upon its formulation by Jim Gray (in his 'Notes on Data Base Operating Systems', 1978), and was then generalized – to larger multiple agent systems – by Leslie Lamport, Marshall Pease, Robert Shostak (in 1980). http://research.microsoft.com/en-us/um/people/lamport/pubs/byz.pdf

As humorously reformulated by Satoshi Nakamoto, in a post on the Cryptography mail list that scrupulously preserves the critical abstract properties of the problem: "A number of Byzantine Generals each have a computer and want to attack the King's wi-fi by brute forcing the password, which they've learned is a certain number of

We imagine that several divisions of the Byzantine army are camped outside an enemy city, each division commanded by its own general. The generals can communicate with one another only by messenger. After observing the enemy, they must decide upon a common plan of action. However, some of the generals may be traitors, trying to prevent the loyal generals from reaching agreement.

The generals must have an algorithm to guarantee that

A. All loyal generals decide upon the same plan of action.

The loyal generals will all do what the algorithm says they should, but the traitors may do anything they wish. The algorithm must guarantee condition A regardless of what the traitors do.

The loyal generals should not only reach agreement, but should agree upon a reasonable plan. We therefore also want to insure that

B. A small number of traitors cannot cause the loyal generals to adopt a bad plan.

§4.09 — 'Byzantine failures' arise when parties distributed within a communication network, containing unreliable nodes, are obstructed from reaching agreement, because they cannot confidently establish among themselves what has in fact been communicated, or from which agents messages have been received. A global perspective appears unobtainable, and local perspective is vulnerable to

---

characters in length. Once they stimulate the network to generate a packet, they must crack the password within a limited time to break in and erase the logs, otherwise they will be discovered and get in trouble. They only have enough CPU power to crack it fast enough if a majority of them attack at the same time. […] They don't particularly care when the attack will be, just that they all agree. It has been decided that anyone who feels like it will announce a time, and whatever time is heard first will be the official attack time. The problem is that the network is not instantaneous, and if two generals announce different attack times at close to the same time, some may hear one first and others hear the other first." The same post explains how a proof of work solution can be achieved: https://www.mail-archive.com/cryptography@metzdowd.com/msg09997.html

It is especially important to note that the BGP formalizes the problem of coordination (in general) as synchronization. As already remarked (in Part One), it articulates a problem whose insolubility, in the context of cosmo-physical theory, coincides with general relativity, spacetime, and the renunciation of absolute succession. A solution to the BGP, therefore, is intrinsically post-relativistic. (Given the restoration of succession to the order of signs that follows from the innovation of the blockchain, the application of the 'post-' prefix in this case has exceptional – and reflexive – conceptual legitimacy.)

See also The Problem of Firing-Squad Synchronization, whose relevance is implicit in its name:

http://motherboard.vice.com/read/firing-squad-synchronization-computer-sciences-most-macabre-sounding-problem

compromise. The extreme difficulty involved in Byzantine communications makes them a model coordination problem, of special relevance to Internet-connected agencies. Crucially, for our purposes here, and beyond, the problem follows upon an assertion of immanence (a critique), since it is defined primarily by the absence of a transcendent tribunal with global insight. None of the 'generals' are able to stand outside the system, call upon an authoritative criterion from beyond it, or even direct their communications around it. Their relation to each other is technically flat (or peer-to-peer). Any solution has to be drawn from out of the system itself – which is to say, from the self-organizational resources inherent to sheer multiplicity.

§4.091 — Nakamoto Consensus, in game-theoretic context, is the name for a solution to the Byzantine Generals' Problem, based upon proof-of-work. By including proof-of-work within each message (hashed block), the generals are able to make the measure of agreement reached – i.e. computational power committed – into an intrinsic property of their communications. Agreement about the message is folded into the message. As blocks are chained, securely, in strict succession, the signal of consensus strengthens. In meeting a reiterated proof-of-work criterion, the blockchain accumulates immanent credibility. It replaces an extrinsic – and intractable – question about the reliability of communications with an intrinsic communication of reliability. Trust is made into the message.

§4.1 — Explicitly acknowledged 'network problems' long pre-exist the electronic era, by centuries, if not millennia. They constitute a guiding thread within what has been called 'the tradition of spontaneous order'.[154] Order is spontaneous if it solves a coordination problem without appeal to any organizational element at a higher – or super-social – level. Spontaneous order, social self-organization, or immanent social process, is thus counter-posed to transcendent social design (from above, or beyond), and to its corresponding theoretical justifications, which amount to a social metaphysics, typically serving concrete functions as guiding ideologies of super-ordinate control. As long recognized

[154] Barry Norman's 'The Tradition of Spontaneous Order' (2002) lays out the intellectual history of the idea, within a primarily legal and economic context: http://www.econlib.org/library/Essays/LtrLbrty/bryTSO.html

Whe abstracted beyond its socio-historical exemplification, and apprehended as a cosmic-philosophical principle, spontaneous order refers to immanent coordination within dispersed collectivities, making it approximately synonymous with 'the science of multiplicities' in general. It designates the systematicity of the system, which can be alternatively formulated as an irreducibility without transcendence, or an immanent non-locality. Whether philosophical, or colloquial, the association of spontaneity with notions of vitality is ultimately arbitrary. Spontaneity is not life, unless 'life' is conceived as the irreducible operation of the multiple as such.

by its opponents, the assertive recognition of this theoretical conundrum cannot be practically dissociated from an implicit political stance.[155]

§4.11 — In the absence of superior guidance, solutions to coordination problems have to emerge, out of – and as – games. This is only to say that cooperation between the agents involved cannot be presupposed, but has to arise from their interaction, if it is – indeed – to appear at all. To assume altruism or solidarity in such cases is a failure to think the problem at all. Coordination is the explanandum. The collectivist dogma is not an answer, therefore, but an alternative to the question. An answer is a trust machine, for which Bitcoin is the model. It is strictly complementary to a minimal presupposition, that of trustlessness (for which it is the solution).

§4.12 — Byzantine generalization extends to the very limit of network communication problems, to the difficulties of establishing coordination within radically dispersed (and thus zero-trust) multiplicities, encompassing non-idealized societies / populations of every variety. It is not, of course, that the concrete existence of trust is simply denied, only that it is rigorously thematized, as a social product requiring explanation – and what counts as an 'explanation' cannot, whether overtly or covertly, merely presuppose what it is called upon to explain. (This demand, as we have seen, is already totally – even ultimately – controversial.) If there is trust, there has to be a trust engine, conceived without pre-existent bonds of trust as a part. At the most abstract level, therefore, this is a topic that

---

[155] Public Choice Theory serves as a reliable proxy for minimalistic, game-theoretical axioms in their directly political application. In her book All You Can Eat: Greed, Lust and the New Capitalism (2001), Linda McQuaig cites a short fable by Amartya Sen, designed to satirize the Public Choice approach: "'Can you direct me to the railway station?' asks the stranger. 'Certainly,' says the local, pointing in the opposite direction, towards the post office, 'and would you post this letter for me on your way?' 'Certainly,' says the stranger, resolving to open it to see if it contains anything worth stealing." Notably, in contenting itself with a satirization of disciplined moral skepticism, this line of criticism is brazenly unembarrassed about its dogmatic structure. Its rhetorical brilliance diverts from its substantive socio-historical meaning, which is the acknowledgment that solidarity is premised on the absence of a question. In other words, it demands, finally, the docile acceptance of an inarticulate presupposition. In this demand is to be found its irreparable weakness, shared by all cultural commitments – typically religious in nature – that are grievously wounded by the very fact of coming into question. A comparable defense of transcendent altruism founded upon the pre-delimitation of critique will be seen in David Graeber's 'everyday communism'. There, too, fatal injury coincides with the beginning of skeptical thought. Since, in this framework of collectivist moral norms, the investigation is the real crime, an intrinsic inclination to totalitarianism proves difficult to control.
There is one, and only one, coherent rejoinder available to the Left on this point. The table has to be reversed, in order for autonomous individuated agency to occupy the role of the explanandum, with its production and reproduction within the collectivity determined as the critical problem. Naturally, the production of individuation within complex adaptive systems would not satisfy this demand, since the presupposition of any such analysis is uncoordinated multiplicity. The Left is compelled to maintain that war is not 'the father of all'. It is darkly amusing, then, that we continue to argue about it.

would have been familiar to the thinkers of the Scottish Enlightenment, as to all those participating productively within the theoretical tradition of spontaneous order. It is exactly this same problem of decentralized coordination (in the absence of any transcendent contribution provided by assumed altruism or common purpose) that has been the essential guideline for realistic social analysis within the 'whig' lineage of descriptive liberalism, exemplified most famously by Adam Smith's figure of the 'invisible hand'.[156]

§4.13 — Evolutionary biology, as a science of emergent networks, has engaged very similar problems from its inception, often with identical tools. This is especially evident in the modeling of ecological equilibrium within large, long-term biological system dynamics, in which the absorption of extinctions defines the 'true network' (by the absence of indispensable nodes). A more recent attempt to formalize such coordination is found in the game theory of John von Neumann, which has itself been effectively applied to biological networks at a variety of scales.[157] The latest – and still rapidly self-transforming –

---

[156] In Smith's most widely-cited words, taken from the Wealth of Nations, the repudiation of assumed altruism is explicit: "It is not from the benevolence of the butcher, the brewer, or the baker that we expect our dinner, but from their regard to their own self-interest. We address ourselves not to their humanity but to their self-love, and never talk to them of our own necessities, but of their advantages." It is only through this theoretical self-restraint that the emergence of social cooperation is critically explained, rather than dogmatically asserted. It is important to note, however, that the recognition of the problem is not in itself a solution. The solution is not a philosophical reservation, but a machine. In Smith's case, of course, it is the market mechanism, understood as a catallactic generator, or engine of spontaneous order, that represents the general (abstract) form of social solutions to novel coordination problems, in a way that remains mainstream within economics up to the present day. When grasped within this framework, it is at least tempting – if perhaps not strictly compelling – to suggest that any purported successor to the market, capable of usurping the role of the market, could only itself be a new iteration of the market. The most prevalent contemporary radical (left) alternative requires that coordination problems, rather than being solved, are instead terminally dispelled. Among those unfashionable vestiges of the Marxist tradition which emphasize the inheritance of capitalistic management practices by post-capitalistic social regimes (as exemplified by Lenin's Taylorism), there is at least the promise of collective action solutions taking the form of legacy cultural resources, although without solid prospect of further innovation in a post-competitive milieu.

[157] The formal application of game theory to evolution dates back to the early 1970s, pioneered by John Maynard Smith and George R. Price, through the theorization of evolutionary strategies (see 'The Logic of Animal Conflicts', 1973, http://adsabs.harvard.edu/abs/1973Natur.246…15S). Since the notion of 'strategy' has an ineliminable telic inflection, this mode of evolutionary formalization can be philosophically-conceived as a diagonalization of biology. A video interview with Smith on the topic can be found here: http://www.webofstories.com/play/john.maynard.smith/42;jsessionid=7E3CA894713888028A8D7066FB3F263E

The preparatory theoretical work of W. D. Hamilton is especially notable in this regard, since it is explicitly focused on the application of Darwinian intellectual tools to subtract the metaphysical pre-supposition of altruism. The rhetorical provocation of selfishness, as seen most prominently in the Hamilton-based neo-Darwinian synthesis of Richard Dawkins, testifies to this project. The 'selfish gene' poses altruism as a problem,

incarnation of this tradition can be seen in the science of 'complex adaptive systems' as exemplified by the research programs of the Santa Fe Institute.[158] In each case, the defining theoretical object is emergent coordination, in which no appeal to any centralized, superordinate, or orchestrating principle is made, unless this can be identified with the system itself, as such. The target of such researches is transcendental order, as captured by the immanent rules of distribution (which are ultimately indistinguishable from the real correlate of mathematics).

§4.14 — Games, strictly understood, therefore, arise under the minimalistic assumptions tolerable to an analytical anarchism,[159] that is: after the methodical subtraction of all presumed coordination, or the conversion of such presuppositions into formal theoretical problems. The implicit critical impulse driving the construction of such research programs is evident. That which might have been asserted, as a transcendent principle, or metaphysical dogma, is to be instead explained, as an immanent, emergent, or 'evolutionary' outcome. Whether explicitly understood in such terms, or not, every such enterprise is a regional application of critical philosophy. Spontaneous order is the correlate of critique. The solution, however, cannot correspond to a philosophical thesis (of any traditional type), or even to a 'machinic proposition' – an engineering diagram, simulation, or protocol – but can only emerge as the synthetic product of such a proposition, when executed. The notion that coordination problems (of significant complexity) can be anticipated in detail by a process of pure ratiocination is a philosophical disease, of recognizably pre-critical type. The idea of the diagonal is not the diagonal.

§4.15 — If the discovery of spontaneous order as a problem corresponds to the execution of critique, it can be formalized through a diagonalization matrix. When the pre-critical opposition of centralized

---

which Hamilton had already productively addressed. This is how transcendental critique reaches social biology, whose compressed name – socio-biology – was, from its inception, a political scandal. Collectivist metaphysics was not slow to recognize the profound intellectual menace – at once ancient and scientifically-renovated – that it faced.

[158]The Santa Fe Institute gathers cross-disciplinary researchers for the study of far-from-equilibrium systems and their emergent behavior, characterized by path dependency, sub-optimality, and massive informational imperfections. Of special relevance to the discussion here has been the pioneering of 'Complexity Economics', associated in particular with the work of Brian Arthur, which provides a disciplined critique of equilibrium models in neoclassical economics. Markets approach equilibrium only in the way that all working machines approach an entropy maximum, without this limit being ever – or even approximately – actualized. See the institute's website at http://www.santafe.edu/

The concrete socio-historical application of such thinking found in Manuel De Landa's (2000) A Thousand Years of Nonlinear History (see bibliography).

[159] Between 'descriptive liberalism' and 'analytical anarchism' – despite the apparent terminological escalation – there is no distinction of serious theoretical significance. 'Order out of chaos' (or at 'the edge of chaos') is the consistent explanatory horizon.

coordination to uncoordinated dispersion is tabulated, it draws a graph isomorphic with the Kantian schema. At the level of the abstract formalism, this latter is echoed with such extreme fidelity that we can borrow from it freely, while switching its terms through a simple hash. Substitute centralization for analysis, decentralization for synthesis, order (coordination) for the a priori, and disorder for the a posteriori. As with the Kantian original, the first diagonal term fails – there is no centralized disorder, any more than there are analytic a posteriori judgments. Centralization is an intrinsically anomalous distribution, necessarily threatened by the prospect of a fall into disorder. Its complementary conception, 'simple anarchy', is no less invulnerable to theoretical dismissal. The previously acknowledged terms, centralized order, and decentralized disorder (like the analytic a priori, and synthetic a posteriori) are therefore preserved. Common sense is not abolished, at least, not initially. In the exact formal place of Kant's invention/discovery of the synthetic a priori, the critique of coordination, too, generates a viable diagonal product – decentralized order. (Quod erat demonstrandum). This is the Great Oblique worked by all realistic social theory since the inception of the modern epoch.

§4.16 — In Cyberspace, the tradition of spontaneous order has been massively accelerated. Classical coordination problems have been reformulated as experimental fields, opened for exploration by the emergence of increasingly-powerful computer simulation tools, and consolidated as practical solutions through the implementation of cryptographic systems and P2P platforms. Philosophical reflection has, to a very considerable extent, been side-lined by technical applications reinforced by far superior criteria of evidence, which is to say: practical demonstration. In the age of electronic information technology networks can be tested as products, and it is possible to ask of a complex idealization, as never before, does it work? This transition, through computer simulation, from explanation to implementation, registers a process of technological envelopment without definite limits. It corresponds to an interminable tide of disintermediation that established institutions of intellectual authority have not yet begun to fear enough.

§4.17 — While institutionalized philosophy has tended to lag the network trend, rather than pioneer it, something that might reasonably be called 'abstract network theory' has nevertheless arisen to become a guiding philosophical theme since the mid-20th century. Among those modes of philosophical writing that have been most influential upon the wider humanities and social sciences, this attention to the distinctive characteristics of networks has been especially notable.[160] Appropriately

[160] The most influential proximal ancestor of current network theory (by far) has been connectionism. This intellectual movement, characterized by an extreme interdisciplinarity, introduced the problems of electronic engineering and distributed information systems into the study of biological, psychological, and social phenomena. Its name was coined by neural net-theorist Donald Hebb, in the 1940s. Rising to prominence from the early 1980s, connectionism has generalized the study of neural networks (or parallel distributed processing) in suggestive coincidence with the rise of the Internet. Its research orientation has been guided by the proposition

enough, this 'discourse' – or dispersed conversation – has no uncontroversial center of authority, stable common terminology, shared principles, or consistent ideology. Its rhetoric tends to systematically confuse advocacy with criticism, and both with analysis, as it redistributes partial insight around a number of relatively tightly-interlocking social circuits (which are overwhelmingly dominated by a familiar set of theoretically-superfluous moral-political axioms).[161] Yet, however deeply regrettable this concrete situation might be considered from the perspective of austere theory, it cannot be simply wished away. Intellectual production itself occurs within networks, and those with greatest promotional capability are among those least optimized for pure intellection.

§4.18 — The cultural systems in which the philosophical (and sub-philosophical) formalization of radically decentralized – or 'true' – networks has emerged, through a multi-decade self-reflexive process, are eccentrically articulated, very partially self-aware, and only weakly integrated. Yet even in these noisy and deeply compromised circles, cross-cut by vociferous extraneous agendas, and subjected only very weakly to a hard reality criterion, convergence upon the rigorous conception of a model

---

that complex adaptive behavior is better explained by the pattern of connections between simple units than by complex properties inherent within concentrated entities of any sort. At a larger scale, connectionism updates the diffuse multi-century current of empirical associationism, accommodating it to the prospects of technological actualization within electronic networks. It is thus marked by a comparative disregard for elaborate symbolic structures, and for highly-organized internal states more generally. The atomic elements of connectionist analysis are linkage modules, supporting emergent systemic behavior. Like cybernetics before it, connectionism outgrew its own disciplinary contour, and dissolved into the sophisticated common sense of the world. (Generalized dominion can be difficult to distinguish from disappearance.) Subsequent attempts to specify a definite 'theory of networks' have been programmatically vaguer, resorting typically to some notional gestures of obeisance in the direction of mathematical graph theory. Much of this work has been seduced by literary temptations, bringing its enduring theoretical productivity into serious question. Most damagingly, in respect to its own capacity for conceptual genesis, the primary analytical discipline of connectionism – programmatic dismantling of mysterious essences into distributions – has been increasingly neglected, and replaced by an arcane cult of whole 'objects' withdrawn from the menace of disintegration.

[161] Axioms are independent, formally-articulated assumptions. Since each axiom is a basic presupposition which cannot (therefore) either be derived from, or support, any other, a set of axioms is an irreducible multiplicity. Consequently, an axiomatic has a characteristic mode of variation, based upon composition from wholly independent parts, which can be added or subtracted with comparative freedom. Because axioms are bedrock elements, their selection demands an irreducible experimentalism. (As a matter of logical necessity, the systems they compose can never determine the characteristics of a missing axiom.) Within a social context, the pursuit of minimal axiomatic systems is ideologically charged, since it corresponds to a contraction of public purposes. The historical disintensification of capitalism has proceeded, as Deleuze & Guattari note, by way of an axiomatic proliferation. Addition of axioms is the way capital has been socially compromised. From a Francophone perspective, this tendency appears as a resilient teleological structure. When the same prediction is extended to Anglophone cultures, in which the recession of classical liberalism remains far more seriously contested, less confident conclusions are advisable.

network has been inexorable. An especially influential example is the rhizome of Gilles Deleuze and Félix Guattari, which provides philosophy with its most rigorously-systematized account of acentric and anorganic order.[162]

§4.19 — A network, in this sense, has no indispensable nodes, entitling it to the adjective 'robust'. Once again, the Internet – at least in its idealized conception – exemplifies such a system. It is typical, at this point, to recall the origins of this 'network of networks' in a military communications project (ARPANET), guided by the imperative of 'survivability' realized through radical decentralization. A network, in what is by now the overwhelmingly dominant sense of this term, is by definition robust. It is constructed in such a way as to tolerate massive disruption. Thus the perennial relevance of the military roots of the Internet. In its practical application, communications resilience has been inseparable from resistance to censorship. Like the basic Internet protocols, Tor ('the onion router') is descended from a military research program, initiated in the mid-1990s by the United States Naval Research Laboratory and subsequently pursued by DARPA. The regularity with which critical elements of state security apparatus are deflected into crypto-anarchist streams, and inversely, suggests a principle of strategic reversibility, in conformity (on one side) with the 'poacher-turned-gamekeeper' phenomenon. Given the prominence of treachery within all rigorously-constructed games, it should not be surprising to encounter this extreme fluidity of partisan identities, in which allies and enemies

[162] Rigorous transcendental formulation of the model network – with all the conceptual ironies and traps this involves – finds its highwater-mark in Deleuze & Guattari's essay 'Rhizome' (which introduces the second volume of Capitalism & Schizophrenia, A Thousand Plateaus). A 'rhizome' acquires facile (contrastive) definition through its distinction from the 'arborescent' schema of hierarchical sub-division. It proposes an absolute horizontality, approached through dimensional collapse, which opposes the rhizome to the tree, reticulation to hierarchical structure, and contagion to heredity. "In truth, it is not enough to say, 'Long live the multiple', difficult as it is to raise that cry. The multiple must be made, not by always adding a higher dimension, but rather in the simplest ways, by dint of sobriety, with the number of dimensions one already has available – always n – 1. (the only way the one belongs to the multiple: always subtracted). Subtract the unique from the multiplicity to be constituted; write at n – 1 dimensions. A system of this kind could be called a rhizome" (ATP 6). When analytically decomposed, the rhizome exhibits a number of consistent, distinctive features. "1 and 2. Principles of connection and heterogeneity: any point of a rhizome can be connected to anything other, and must be. … 3. Principle of multiplicity: it is only when the multiple is effectively treated as a substantive, 'multiplicity', that it ceases to have any relation to the One as subject or object, natural or spirtitual reality, image and world. Multiplicities are rhizomatic, and expose arborescent pseudomultiplicities for what they are. … 4. Principle of asignifying rupture: against the oversignifying breaks separating structures or cutting across a single structure. A rhizome may be broken, shattered at a given spot, but it will start up again on one of its old lines, or on new lines. You can never get rid of ants because they form an animal rhizome that can rebound time and again after most of it has been destroyed. … 5 and 6. Principle of cartography and decalcomania: a rhizome is not amenable to any structural or generative model. … [The map] is itself a part of the rhizome. …" (ATP 7-13). Manuel DeLanda proposes the term 'meshworks' for such systems of flat, heterogeneous, interconnectivity, which he opposes to (comparatively rigid and homogeneous) 'hierarchies'.

switch positions. The figure of 'the hacker' is notably liminal in this regard, representing – simultaneously – an ultramodern incarnation of the outlaw, and a skill-set indispensable to effective formations of contemporary power. At its highest levels, strategy is a matter of 'turning'. This is the diplomacy intrinsic to strategy (and thus to war), once the latter is liberated from the strait-jacket of its political – or Clausewitzean – determination, and released into a conceptual space bounded only by a transcendental horizon. Friend and foe are defined within the great game, rather than outside, by its transcendent (political) frame. There can be no assumed parties at the transcendental level of the game, where not only every alignment, but any constitution of agency is itself a 'move'. Agencies are pieces, consequent to strategic decisions. However tempting it might be to dismiss such considerations as arcane, they are already being condensed by commercial crypto-systems as practical problems. In regards to their legal form, modern business corporations have been synthetic agencies for well over a century. In the emerging epoch of Digital Autonomous Organizations ('DAOs'), whose economic and military implications are yet scarcely glimpsed, this status advances from a matter of legal definition to one of software implementation. It consummates the historical triumph of code. At the end, as – invisibly – from the beginning, the transcendental subject is fully immanent to a plane of strategic production. As will be repeatedly noted, on the crypto-current the security criterion is primary, providing system dispersion with its principle. This suggests, as an ideological generalization, that there is no basic 'trade-off' between liberty and security. Rather, it is through security (alone) that liberty establishes its reality. The term "crypto-anarchy" condenses this conclusion into a program.

§4.191 — Such invocations of the strategic investment in distribution and redundancy, however predictable, remain conceptually productive. They are especially valuable as a corrective to modes of discourse – typical among contemporary humanistic studies – which tend to haze the harsh selective or eliminative function of critique into a vapid metaphor. It is the military ancestry of the Internet that is tacitly referenced in the celebrated maxim of John Gilmore (1993): "The Net interprets censorship as damage and routes around it." In order to save command-control, it was necessary to fundamentally subvert it.

§4.2 — War games are built into the fabric of the Internet. This is at once a matter of uncontested genealogy, and of an as-yet only very partially explored transcendental-strategic landscape.[163] As we

[163] A 'transcendental-strategic landscape' – constituted by an absence of transcendent legality – corresponds to a the concrete problem of anarchism, in the sense this term is understood by realist international relations theory (IRT), and realist strategic analyses more widely. That is to say, it poses issues of security without any possibility of appeal to superordinate authorities (or authoritative referees). Hobbesian political theory, in which "the war of all against all" is exposed by a secular 'Death of God', establishes itself upon a negative foundation. Leviathan begins from that which cannot be relied upon. Whether domestically, or internationally, the transcendental (i.e. ultimate) theater in which powers meet is defined by the subtraction of any original commanding unity. Security is thus theoretically constituted as a problem, corresponding to a primordial lacuna. Since it is not given, it has

have seen, according to one (comparatively mathematicized) formal meta-description, Bitcoin arose as the solution to such a game – the Byzantine Generals' Problem. This immediate context is so closely tied to the achievement of the Bitcoin Protocol, by those most closely associated with its formulation, that it has been widely adopted as a definition.[164] Yet even if the solution to Byzantine coordination establishes the game theoretical significance of Bitcoin, it does not exhaust it, even remotely.

---

to be positively produced, and it is in the identification of this practical conundrum that IRT isolates its proper object of study. On the Internet, as in the international arena, it is only upon such a cleared, immanent plane, that a true game can take place. It cannot be sufficiently stressed that the conflictual field is not – as its critics have over the centuries necessarily insisted – a positive presupposition, but rather a mere default, assuming only original diversity under the conditions of an absent integral authority. Despite its manifest tendency to decay into a Utopian projection, the perpetually-regenerated credibility of anarchism is founded not upon its transcendent aspiration, but upon its transcendental problematic. Given only war, how is coordination possible?

[164] While the definition of Bitcoin as a solution to the Byzantine Generals' Problem remains controversial, the principal objections to this description can reasonably be described as arcane. As Oleg Andreev notes, in a brief but valuable discussion of the proof-of-work solution, any actual production of communications integrity is compromised in its logical purity by practical limits (bounded by cryptographic intractability). In other words, precisely because it is transcendental, Nakamoto Consensus cannot be transcended even by its own proof. The limit is set by the working machine. This is a matter of extreme generality. While persistently – and even essentially – tempted by Platonism as a heuristic, mathematical procedures require instantiations which are transcended only in conceptual principle, which is to say: hypostatically, through appeal to transcendent grounds whose authority is purely ceremonial. Compelling demonstration already returns the problem to the machine, and its real potentials for effective execution. Operationalizations are not, in reality, superseded, or subordinated, but only (at most, and typically) bracketed, or abbreviated, and thus – again, in reality – assumed. The credibility of the Idea refers to potential demonstration. The keystone of proof says nothing else. Untested trust is an oxymoron. It would be a grave error – though an all-too common one – to seek an epistemological demotion of 'credibility' to the psychological category of 'mere opinion' while admitting this. Credibility is basic. Without it, no truth has been earned. This is the meaning of deduction in its critical and realistic sense. What lies beyond is metaphysics, enthroned upon arbitrary assertion. Irrespective of any extravagantly-promised protections, there is no confidence – no security – to be derived from that. However much Bitcoin has to appear as an Idea, therefore, it is irreducible to one. It cannot be expected that this stubborn factuality is susceptible to comprehensive dissolution into the form of the concept, still less that it will be fully factored into a security analysis. On the contrary, realism predicts its chronic idealization (i.e. misidentification). In this respect, philosophy is a security hole (proposing answers in place of solutions, or dispelling threats only in ideality), if not – in its institutional form – a particularly serious one. … Since insecurity has no adequate idea, it cannot be speculatively resolved. This point of elementary realism calibrates the appropriate level for confidence in philosophy (and does so in actuality, not only in principle). Philosophy is not seriously entrusted with keeping anything safe. Its invitation to live dangerously is – in this respect – a sensible concession to the inevitable. The untested or – still worse – untestable model need not be about danger to be dangerous. Armchairs are places where things can go wrong without limit. … The Byzantine Generals do not secure themselves through a speculative philosophy, but through a robust procedure. Did they have a 'good plan' before testing it? (It could, at most, only appear so.) … Security concerns only risk, which is never merely a conceptual possibility, but always a matter of discovery. The

§4.21 — Bitcoin is both less than, and more than, a mathematical theorem, because it remains a game in process, and also a meta-game. There is an irreducible informality to Nakamoto Consensus, insofar as it remains open, or unsettled, at multiple levels. As a concrete procedure, it effectively invokes a sociotechnical process of uncertain destiny within its demonstration, making it ill-suited to the purposes of mathematical proof.[165] If the mining procedure – rather than the reward criterion – could be fully specified in advance, and thus support predictive deductions, it would do no work. Incentivization – in every case – presumes non-deducible outcomes. Bitcoin, like all incentive systems, is a synthesizer. It produces a social process, as an event, and an arena (or agora), and thus advances experimental game theory, through an artificial environment especially conducive to the emergence of spontaneous ('trustless') coordination. Concretely, this space is a hothouse for business innovation, which constitutes the leading – and perhaps still 'bleeding' – edge of microeconomics, where

---

fact that Bitcoin appears to be a 'sound idea' is not finally separable from its concretely-elaborated existence as the most rigorously-tested trust mechanism in the history of the earth. …

http://nakamotoinstitute.org/mempool/proof-that-proof-of-work-is-the-only-solution-to-the-byzantine-generals-problem/

Ian Grigg argues that the classic coordination problem has been displaced, into the far more protean quandaries of a 'dynamic membership set'. Critical Bitcoin security challenges, most specifically that of the Sybil attack (based upon identity proliferation), entirely exceed the horizon of the BGP. "If Bitcoin solved the Byzantine Generals Problem, it did it by shifting the goal posts." http://financialcryptography.com/mt/archives/001522.html

[165]A machine with integral incentives necessarily combines formal – or formalizable – and informal elements. To a still-imperfect approximation, but with definite teleological inclination, Bitcoin is politically closed, while commercially and industrially open. In this respect it echoes – and even escalates – the ideal of the arch-liberal (capitalist) social order. The mining objective is exactly specified. The criterion for mining success, compensated automatically in bitcoins, is a hash of the current (problem) block whose nonce begins with a definite number of zeroes (a figure adjusted for difficulty). Despite this extreme formality, the mining procedure involves both chance and – more importantly – innovation. Bitcoin hashing is formally constrained to trial-and-error methods, with probabilistic outcome. In the words of the Bitcoin wiki: "The probability of calculating a hash that starts with many zeros is very low, therefore many attempts must be made." Everything beyond the product specifications (the puzzle solution) is left open. In particular, the production techniques are left undetermined, and thus open to industrial innovation. See: https://en.bitcoin.it/wiki/Mining

Similarly, and even more markedly, the commercial opportunities opened by the protocol are uncircumscribed. The 'value' of the Bitcoin currency, in the broadest sense, is settled dynamically outside the blockchain, through a radically decentralized and uncomputably complex dynamic of exchange. (The exchange process – catallaxy – is the computation.) The protocol sets the total stock of bitcoins, without predetermining their distribution (between agents) or price (when denominated in any other financial medium). The value of the currency cannot be derived from the rules determining its quantity. It is synthetic. Bitcoin's productivity lies in what it leaves open, even as its integrity is secured by what it closes.

generalized theory and practical enterprise have yet to dissociate. The boundaries of the Protocol, while strictly defined in certain respects, are profoundly unsettled in many others, and there is no strongly economical way to settle them. 'Where does it end?' is a question that has to be explored historically, without conceptual short-cuts, by an irreducible synthetic process. It is thus roughly modeled by the Bitcoin mining procedure, where the ineluctable necessity of trial-and-error – or uncompressible method – precludes all possibility of rapid philosophical (i.e. purely conceptual) resolution. Bitcoin is a game, and is like history, in that it cannot be worked out without being actually played – or hashed.

§4.22 — Real games are far-from-equilibrium processes that approach formality without actualizing it. They consume freedom – by contracting discretion – with every move that is made, and prolong themselves by reproducing it, in a circuit. Only insofar as this holds do they include incentives, as an irreducible teleological element. The open-ended mechanization of purposes is the diagonal along which they proceed. When apprehended at sufficient scale, this process is equivalent to industrialization. With the arrival of Bitcoin, money is – for the first time – subsumed into industrial revolution. A great historical circuit is cybernetically closed (which does not mean finished, but something closer to the opposite, i.e. initiated). Techonomic fusion – the singularity guiding modernity's convergent wave – can for the first time be retrospectively identified. On Halloween 2008, the end began. What modernity has been from the start was then sealed.

§4.23 — Friedrich Nietzsche's On the Genealogy of Morals dedicates itself to describing how man became "an animal with the right to make promises". The story has turned out to be even longer and more intricate than his work anticipated, but the quasi-paradox there explored, knotted into the concept of debt, retains its pertinence into our time. How is a free commitment possible? Bitcoin attends explicitly to the same problem. "Transactions that are computationally impractical to reverse" – of the kind Bitcoin facilitates – constitute voluntarily-adopted mechanized commitments, immunized against all vicissitudes of will. Since algorithmic irreversibility enables an inability (or disables an ability), there is much here that seems self-contradictory upon superficial consideration.[166] Yet such a facility – or, indeed, power – of self-limitation is already fully implicit in the word 'bond', and in any serious

[166] Self-binding is a classical problem, epitomized by the strategy adopted by Odysseus in his passage past the Sirens. Anticipating an irresistible seduction, he commits to a decision which he then – by crude socio-technical means – renders irreversible. Within game theory, the same problem is a central preoccupation. It is admirably summarized by Scott Alexander: "… it sounds weird to insist on a right to waive your rights. Isn't that more of an anti-right, so to speak? But … read your Schelling. In multiplayer games, the ability to limit your options can provide a decisive advantage. If you're playing Chicken, the winning strategy is to conspicuously break your steering wheel so your opponent knows you can't turn even if you want to. If you're playing global thermonuclear war, the winning strategy is to conspicuously remove your ability not to retaliate, using something like the Dead Hand system. Waiving your right to steer, waiving your right not to nuke, these are winning strategies; whoever can't do them has been artificially handicapped."

sense of commitment. A contract is an expenditure of liberty. The motto on the coat of arms of the London Stock Exchange, Dictum Meum Pactum ('My Word is My Bond'), extends the principle – by etymological suggestion – to the most elementary cases of formalized social association ('pacts'). Society is a game, which arises from its ragged edges. The deal describes the frontier.

§4.24 — During a 'Fireside Chat' on 'Bitcoin and the Future of Payments Technology'[167] Larry Summers makes exactly the same point:

This is an area that I think is rich with irony. … the single most important development in the history of the common law corporation was when the legal principle that it could be sued was established. And you might ask: why was it good to be sued? Well, because if you can't be sued you can't enter into a binding contract, and only when you could enter into a binding contract could you carry on commerce in a major way.

§4.25 — Bitcoin subtracts the option to defect (or double spend). The protocol sets the rules of a new game, in which the violation of contract ceases to be a permissible 'move'. By automatizing this constraint, and thus withdrawing it simultaneously from the realms of contractual agency and regulatory oversight, Bitcoin instantiates algorithmic governance in its own, specific domain. Human discretion is displaced to the boundary of the Bitcoin commercium, and into the zones of meta-decision (for economic agents and authorities respectively) whether to enter or permit Bitcoin. These dilemmas introduce a knot of complex and typically highly-recursive games that can be grouped under the umbrella term 'Bitcoin politics'.

§4.3 — To propose that the political controversy associated with Bitcoin can be expected to escalate in approximate proportion to the crypto-currency's success, as quantified by its total market value, is unlikely to provoke feverish dispute. Yet such distribution concerns are comparatively trivial – at least at the level of political principle – when set alongside the questions of sovereignty that crypto-currency raise. Bitcoin is a limit strategy of depoliticization, which – at the cliff-edge of historical irony – announces an ultimate political contest. No stroke can be more intensely politicized than one threatening to sweep away a whole field of political decision-making. As a purely ideological challenge, therefore, Bitcoin organizes a terrain of political antagonism in advance, provoking (in reaction) a defense of politics of unprecedented conceptual purity. Crypto-currency self-regulation elevates the menace that has long-spooked left-articulated[168] political interests under the guise of the

[167]The quote is extracted from this video record: https://www.youtube.com/watch?v=UVGq0zaZsNg&feature=youtu.be

[168] From a certain perspective – which is not itself isolable as a 'left-wing' or 'right-wing' theoretical orientation – there is no right-wing politics. The political, by its own dialectical logic (of organized controversy and reconciliation), can only reach conclusion on the left. Insofar as social process conforms to a structure of

autonomization of capital to an almost parodic height. It ceases entirely to be answerable. Dialectic loses all purchase. This is widely grasped, even though the thing itself cannot be. Bitcoin is a game-changer.

§**4.31** — It can easily become confusing to talk about games. An allusion to non-seriousness need not be a great problem – what, after all, is seriousness? More obfuscating is the invocation of rules. Insofar as a 'game' is thought to be essentially rule-bound, the train of associations is guided in a direction that is radically misleading. Games are defined by rules, but they are determined far more informatively, by the absence of rules than by their presence. The game occurs in the unruled area – and insofar as further subtraction of rules can be achieved, the game is thereby intensified. Rules set the boundaries of a game, but the strategies that compose the actual (or executed) game's positive characteristics substitute for a rule. They are synthetic. There is a difference, therefore, between transcendent and immanent principles, or – more strictly – between rules of transcendent and immanent genesis. The former, determined in advance of 'play', set fixed parameters, or ideal competences, comparable to axioms and exposed in advance to analysis. The latter emerge – synthetically – from the performance of the game, as demonstrations, or discoveries. A game is always improved, qua game, when its set of transcendent principles is reduced, through conversion into immanent principles (or emergent outcomes). While there is a Bitcoin protocol, Bitcoin is not reducible to it. Bitcoin is rather the outcome of being 'played', in conformity with those rules that the protocol – firmly but non-comprehensively – establishes.

---

argumentation, its sinister destination is assured originarily, as the Left Hegelians were the first to distinctively, if only implicitly – and not (of course) at all uncontroversially – comprehend. For the right, agreement to pursue the social argument is already to lose it. The position of the right, most definitively in the case of established property distributions, is that there is nothing to discuss. The absence of any opening for discussion is what property rights ultimately mean. Whatever is unable to escape argument remains unsettled, framed by an implicit re-distribution which merely awaits actualization upon the collective horizon that is defined by the final scope of controversy or – restated exactly – the political totality. Under such conditions, which are conceived by the left as universal, private property is only ever held on trust, as a contingency of revisable political arrangements (or a debatable social allocation). Controversy – even ideological controversy – falls short of the difference referenced by autonomy. From the side of privacy, there cannot be any encompassing negotiation or 'dialectical relation' – between the public and the private. Privacy, private interest, cannot be protected – or even rigorously articulated – within a sovereign public forum. As soon as it makes a case for itself through political argument, or ideological commitment, which could only ever be ambiguous, it submits to the final authority of the conversation, and thus to the collective. Its sole defense lies in exemption from politically-significant social discussion, an avoidance that is not (merely) anti-dialectical, but positively exo-dialectical, requiring something other than opposition. Non-dialectics is not a higher level of argument, but an escape from the oppositional relation (into Outsideness). This exit from the political sphere is concretely instantiated by hard crypto-security. Bitcoin epitomizes such a meta-strategy. (Hence the extremity of its political-economic provocation.)

§4.32 — When games turn back upon their own rules, absorbing them into strategies as variable outcomes (of performances), they pass into politics, on their way to war.[169] It follows that politics makes itself difficult to talk about, since the analytical frame necessarily becomes a disputed frontier. If the games that matter were comprehensively structured by uncontested explicit rules, they would not be happening at all. There would be no field of contestation, and thus no contest. Loyalty to the game, as such, has become the axis of potential defection. Strategies marked as 'cheating' within a commercial context are elaborated, and acquire a very different self-representation, as resistance. To thus identify game-theoretic defection with social solidarity – or collective refusal – demands a thorough re-organization of meaning, and eventually nothing less than a cultural revolution.

---

[169] Whatever the positive semantic associations accumulated by the word 'war', its most rigorous meaning is negative. War is conflict without significant constraint. As a game, it corresponds to the condition of unbounded defection, or trustlessness without limit. This is the Hobbesian understanding implicit in the phrase "war of all against all" (bellum omnium contra omnes), in which "the state of nature" is conceived – again negatively – through a notional subtraction of limitation. Treachery, in its game-theoretic sense, is not a minor theme within war, but a horizon to which war tends – the annihilation of all agreement. Reciprocally-excited mutual betrayal in departure from an implicit 'common humanity' is its teleological essence. It is worth emphasizing this point, in the interest of conceptual integration. The game-theoretic definition of mutual military escalation – and thus the inner-principle (and intrinsic motor) of war – is reiterated double-defection. This is a conclusion explicitly rejected by Carl von Clausewitz is his treatise On War, even as he acknowledges the cybernetic inclination to amplification (or "tendency to a limit") which drives it in the direction of an absolute. "War is the continuation of politics by other means," he insists, because it is framed by negotiation (book-ended by a declaration of war, and a peace treaty). According to this conception, it is an interlude of disagreement, which nevertheless remains irreducibly communicative, and fundamentally structured by the decisions of sovereign political agencies. Even as it approaches its pole of ultimate extremity, it never escapes its teleological dependency, as a means (or instrument) of rational statecraft. There is a stark arbitrariness to this assumption. If there is an inherent limitation to military escalation, restricting it within the bounds of political direction, Clausewitz never explains its principle. The reduction of war to instrumentality is not immune to criticism. Philosophical radicalization, alone, suffices to release war from its conceptual determination as 'the game of princes'. Sovereignty has military, rather than political, foundations. Hence the reversal of dependency, which is captured by Michel Foucault's notorious inversion of the Clausewitzean formula into the maxim: "Politics is war by other means". If political sovereignty is ultimately conditioned by the capability to prevail upon the battlefield, the norms of war can have no higher tribunal than military accomplishment, in reality. No real authority can transcend survival, or survive a sufficiently radical defeat. There is thus a final incoherence to any convinced appeal to the 'laws of war' (when inclined to the objective, rather than subjective, genitive). Quite simply, unless war restrains itself it is not restrained. Nothing is able to transcendently impose upon it. Any realistic conception of 'limited war' subsumes that of 'war lawfully pursued' (with the latter properly categorized as an elective limitation). Unless war has a master, 'just war' is ontologically restricted to the status of a tactic. War has no master. There is strictly nothing that could be asserted with greater confidence. "War is the Father of all things," (Πόλεμος πάντων μὲν πατήρ) Heraclitus asserts at the dawn of philosophy. Cormac McCarthy's Judge Holden is more succinct still: "War is God." If it has ever seemed otherwise, it is because the essence of war – as Laozi (among others) has told us – is deception.

§4.33 — A very brief digression into the articulation of politics – which is also the politics of articulacy – imposes itself at this point, beginning with the 'structural linguistics' of Ferdinand de Saussure,[170] a theoretical framework which attained a voguish authority over the politicization of commanding cultural institutions during the second half of the 20th century. In the non-STEM fields of the western academy, in particular, the influence of these ideas is difficult to exaggerate. A 'structure' in this specific theoretical sense is a system of differences – or significant discriminations – which distributes meaning within a hierarchy of contrasts. Its semantic atoms are produced through relations of reciprocal determination, most commonly represented by 'binary oppositions'. Within an opposition of 'A' and 'B', 'A' is 'not-B' and 'B' is 'not-A' – and this exhausts their production of meaning, when extended across the concatenated differentiations of the linguistic totality. Saussure insists there are no positive terms. Signs acquire significance only through their distinctions, as these are applied to an intrinsically amorphous world, sub-dividing it into 'signifieds' – reciprocally demarcated plots or allotments of meaning.[171]

---

[170] Saussure's A Course in General Linguistics (1916) was compiled from lecture notes (by his students Charles Bally and Albert Sechehaye). Its historical coincidence with the origin of macroeconomics merits explicit note. The United States Federal Reserve System, established on December 23, 1913, had scarcely begun operating when Saussure delivered his lectures on the arbitrary nature of the sign. In both cases, a spontaneous order falls under a commanding narrative of discretion, and management of value. The directing impulse – in modern no less than ancient parlance – is Promethean. The resonances between the new monetary order and structural semiotics are not limited to their implicit managerial orientation. They proceed in concert to the horizon of collective-volitional anti-naturalism (dismissing all intrinsic assets and positive terms). It would not be reckless to predict that the theoretical foundations of the macroeconomic epoch will be retrospectively understood as monetary structuralism (and – in its deutero-decadence – 'post-structuralism').

[171] Grasped in terms of its abstract principle, Saussurean 'structuralism' (i.e. semantic constructivism) is the dominant paradigm – or meta-paradigm – governing the conceptual order of the postmodern western academy. 'Post-structuralism' has only deepened its dominion. Because its programmatic anti-naturalism dovetails so perfectly with the institutional task of defensive demarcation, over against the ascendant hard sciences, it has acquired a super-biblical authority within the modern humanities and soft 'sciences'. This enterprise of demarcation is no younger than the modern university itself. It acquires 18th century articulation as a conflict of the faculties. The extraordinary importance of structuralism as a cultural influence thus descends from its (implicit) status as a vulgarization of transcendental philosophy, facilitating the general application of critique across the entire domain of humanistic study. By theoretically severing the production of articulate meaning (phenomenon) from an inaccessible – formless – reality (or "thing-in-itself"), it established constructivist principles applicable to the general study of signs, sparking a 'semiological' revolution of extraordinary influence. De-naturalization became a cognitive reflex, and a matter of zealous dogma. The 'natural' – as that which eludes political adjudication – is identified as the mark and mask of conservative obstruction. Revolutionary denaturalization approaches tautology. In its most rigorous formulation, systematized by Jacques Derrida under the flag of 'deconstruction', critical anti-naturalism proceeds through a series of methodical steps. It first identifies a privileged norm (metaphysical object) within the transcendental matrix of semantically-productive differences,

§4.34 — If we ask – in the degraded ideological mode (alert only to power-oriented, motivated reasoning) – why this type of linguistic theory rose to such an extraordinary position of cultural dominion, suspicion properly falls upon one particular assertive presumption: the arbitrary nature of the sign.[172] As the mantra of choice for a radically-generalized anti-naturalism, this doctrine lays down

---

before successively inverting the conceptual hierarchy (through the dialectical performance of antinomy), and then liquidating it under the evanescent label of a non-representable absolute condition of production (which never bears this name). Critique is thus regenerated as pure schematics of cultural subversion. Notably, it is weaponized primarily against structures of conceptual articulation, and only very derivatively against their (hazily envisaged) institutional manifestations, such as 'patriarchy' or 'neocolonialism'. Deconstruction is thus to be contrasted against more thoroughly-materialized tendencies of critique, in which the supreme instance of social metaphysics is stubbornly identified as the state, and the institutionalization of 'trusted third parties' in general. When critique is subjected to academic professionalization as a bureaucratically-regularized deconstructive practice, the state ceases to be its target, and becomes its occult-transcendental agent. Fortunately, the subordination of critique to the agenda of what Schopenhauer describes bitingly as 'university philosophy' has been far from complete, and increasingly looks uncompletable. As it advances, it incentivizes route-arounds. This opportunity has already begun to be seized.

[172] The 'arbitrary nature of the sign' is treated at once as a sacred and scientific principle by the descendants of the structuralist revolution. The idea is, however, properly understood as a dogma. It is not argued, but assumed. The most firmly-grounded line of criticism is directed towards the hyperbolic formalism it exemplifies. In dissent, it might be noted that the phonic and graphic materials employed for linguistic encoding are no more 'arbitrary' than comparable monetary media. As we have seen, there has been nothing arbitrary about the selection of precious metals as money. Rather, they were advantaged by definite, positive (non-formal) qualities. Linguistic signs are no different in this – abstract – respect. For instance, they need to be compact, memorable, and executable, as well as distinctive. They are often positively suggestive, in ways partially captured by the over-stressed term 'onomatopoeia'. Much basic vocabulary seems to be genetically promoted (i.e. to some remarkable degree 'innate'). Stutter stutters. Slithering is self-decoding. The non-arbitrariness of the sign is typical. Nothing much beyond ideological convenience says otherwise. Structuralist methods, then, are not discoveries, but motivated impositions. They suppress 'positive terms' as a matter of principle. Obdurate substantiality of the semiotic medium is frictional. It offers impedance. It gets in the way of something. The anti-structuralist criticism is thus drawn into a more symptomatological mode of suspicion, as soon as it is asked: What is being obstructed? What is the plan? Social construction is the discursive complement to fiat currency. In both cases, the politicization of values is untethered from natural constraint (with all reference of the former to the latter denounced as pre-critical error). What the figure of the 'gold-bug' is to the Keynesian financial establishment, the 'naturalist' is to the social-constructivist critic. In each case, there is a (supposed) fetishization of a 'barbarous relic', eclipsing a process of collective, cultural-institutional fabrication. Within the overtly dominant strand of the critical tradition, what occurs is a definite triumph of the will. The thing-in-itself is implicitly identified as practical substance, manifesting the world out of mass volition. Contextualized in this way, all objectivity is cast as essentially modifiable, in accordance with political decision. 'Nature' is denounced as the mystified representation of alienated collective desire. This is sheer Schopenhauer, in an ironical, communistic configuration. The deep structure of critique has pre-programmed it, by setting the topic for a multi-century project of institutional absorption (whether conceived as a process of statist-Hegelian formation applied to critical-Schopenhauerean matter, or as a political-institutional interiorization of the thing-in-itself). There are,

a welcome mat to politicization, and has thus contributed immensely to the self-consciously Gramscian reconstruction of the western academic humanities and social sciences during the mid- to late-20th century. What was being said about signs in this context and what was being done with them evidently interconnected, but only indirectly. The highly-formalized – and thus conveniently replicable – ideological signaling system that had been put in place by this cultural revolution established the rules of a new game, or rather, submerged those of the old one. The new dispensation was not to be predicated upon the formulation of protocols, but upon the management of faction. Friend-foe identification procedures rapidly attained uncontested authority, invigorated by blind convergence upon the essence of the political (as found in orchestrated in-group / out-group antagonism).[173] The practical economy was impressive, and in fact irresistible. To obstruct the process of identification was to identify oneself (as hostile), and thus to auto-eliminate the obstruction. In the name of an overturning of 'privilege' the new order of institutional-cultural meaning had privileged absolute, unchecked (or 'arbitrary') political discretion in the last instance, and through retro-projection. There had never (any longer) been anything but politics. The political collectivity alone decides, overcoming its alienation or false-consciousness in the dissolution of objective nature and complementary recognition of its own (naturally and traditionally) untrammeled power of reality-production. This commitment defines the Left, in its critically-coherent manifestation. It describes a generalized absorption into politics that the Gramscian (or Left-hegemonic) academy self-consciously facilitates, under the banner of the arbitrary or illimitably contestable sign. Across large swathes of the contemporary academy, such thinking has manifestly triumphed. Academic authority, and even the strictest kinds of academic credentialization, has been increasingly digested by it. Everything that organized intellectual activity touches upon is to be democratically challenged and policed, under the direction of the dominant – mass – faction, though (of course) through its institutional representatives. All values are resolved into ethico-political obligations, and thus submitted to inflamed moral struggle

---

however, definite indications that the zenith of this assimilation process has passed, among which the emergence of Bitcoin – entirely outside it – is exceptionally striking. The dissolution of precious metals into a bureaucratic apparatus of macroeconomic expertise was not supposed to end this way, with techno-synthetic money bypassing the state and its orbital institutions. The conversion of money into a tool of centralized social administration led to another money. "We need a better barbarous relic," the crypto-anarchist whispers had long insinuated, but they had been pitched-down below the threshold of public audibility. According to all accredited perception, 'improvement' had been heading in an entirely different direction. That is why Bitcoin performs, at once, a capitalist comedy and a socialist tragedy, attained through a surprising reversal of apparently-settled fortune. The mediation of naturalism through traditional cultural institutions can expect similar (or more generalized) relegation. Decentralized commercial genomics would be one relevant field to watch.

See: http://marginalrevolution.com/marginalrevolution/2011/10/who-first-called-gold-a-barbarous-relic.html

[173] The point is Schmittian, but the Left has been far more adept at assimilating it than the Right. https://pdflibrary.files.wordpress.com/2008/02/schmitt_polittheology.pdf

(recognizably post-theistic Protestant in type). The institutional consequences have been starkly evident. Polemic inflates along an axis of raw signal-amplification – which is finally shouting. When Bitcoin secures itself against voice, this is what it effectively succeeds at ignoring.[174] No shouting can conceivably be loud enough to perturb it. Like the crew of Odysseus, bypassing the Sirens, its ears are sealed. A certain strategic desensitization approaches its limit.

§4.35 — An overtly differential – and volatile – polarization of meaning follows upon the politicization of signs, when they are taken up as markers of organized antagonism, functioning as rallying points and signs of aversion, comparable to heraldic devices on a medieval battlefield.[175] The partisan adoption of linguistic signs, as 'flags', destabilizes them in peculiar ways. Structural determination is systematically aligned with faction, and subsequently warps in accordance with political vicissitudes. Ideological terms are driven into unusual migrations of meaning, through rapid twists, turns, and complicated zig-zags, which model – non-coincidentally – a dialectical process of development, in which everything becomes its opposite, on the way to absorption into totality. The word 'liberal' (and its associates) – for important reasons – provides the most remarkable case, pressed into crazed meanderings across nearly the entire field of political significance, even as this domain asserts itself as all-encompassing. 'Liberal' and 'anti-liberal' are terms that have evolved – or degenerated – to such a point that they have become near-perfect synonyms, serving only as indications of evanescent factional identification. The meaning of 'federalism' has undergone a comparable process of structural devastation. It is natural then, to expect the signs of pure political polarization to manifest an extreme degree of semantic instability, and this is precisely what we find with the words 'right' and 'left' (in their political usage).[176] Unsurprisingly, these words are regularly denounced – from all sides – as mere

---

[174] "How did we get from the academy to the economy?" it might be asked. The social function of academically-credentialized expertise does that, when it operates within an institutional context of super-economic oversight. Once again, in the great scheme, macroeconomics is the bridge. As a central trust-management institution (historically supplanting the role of the church), the university is clearly situated in the crypto-currency flight-path.

[175] For an illustration of tribal polarization in the realm of political signs, it would be hard to improve upon the example identified by this pseudonymous Internet comment, on the topic of the 'Obamaphone': "Do you find it entirely implausible that the program was promoted under the Obama administration, that it being Obama's administration doing the promotion helped it go viral in the recipient community, and that all the reasons it went viral as a positive thing for the recipients made it go viral as a negative thing for conservatives? … There's no distortion, no lying. What one side sees as a good thing is PRECISELY what the other side sees as a bad thing." http://slatestarcodex.com/2015/09/03/theses-on-trump/#comment-233889

[176] The Left / Right distinction is regularly derided as a mere anachronism, without consistent meaning beyond its historical reference to 'the seating arrangements of the pre-revolutionary French National Assembly'. Relatedly, the notion of a 'modern right' is easily dismissed as a compact self-contradiction. Yet, insofar as modernity has exhibited internal ideological polarization – rather than merely incarnating the triumph of the left – some such distinction is inescapable. The intrinsic arbitrariness of the left-right terminology is in this respect

triggers for conflictual group dynamics, and as an invitation to intellectual chaos. The semiotic in-group / out-group rituals of micro-sociology have a far firmer grip on such terminology than that enjoyed by political philosophy. As is typical of political language, these words have become signals of group belonging, while only very secondarily preserving the capability to designate any definite grounds for the social or cultural categorization in question. Flagged allegiance ('us' or 'not us') swamps – and drowns – all positive meaning. Insofar as the intrinsic interests of philosophy are concerned, therefore, it is impossible to over-emphatically denounce the cognitive destructiveness of partisan identification. This is the basis for the admirable maxim adopted by the rationalist website LessWrong: "Politics is the mind-killer."[177]It is also why the very idea of intrinsic philosophical interest has to be systematically derided from the side of politics (typically, as the mask for a hidden or crypto-politics).

---

an opening for productive abstraction. It is proposed here that 'leftwardness' on the principal political dimension is measured by the degree of attachment to a presumption of altruism, typically identified with the possibility of a comparatively unproblematic political expression of collective purpose. The 'right' is thus naturally identified with a constitutive cynicism. Given its apparent reference to definite incentives, the Marxian (or 'scientific socialist') conception of 'class interest' might be taken as a repudiation of altruistic presumption from the left. In this – crucial – case, however, the perfect coincidence of individual and collective interest attributed to the universalized – and thus simply 'human' – classless masses that have descended from capitalism's industrial proletariat serves as the proxy for an altruistic orientation, structurally indistinguishable from that traditionally promoted in a more unapologetically sentimental and religious vein. The expectation that a history of industrial cooperation will have fully educated mankind out of all narrow self-interest is, at the very least, a bold one. Dreams of a 'new man' have been consistently disappointed, however elegantly they have been justified by socialist philosophy, within the historical context of concrete initiatives promoting collectivist economic reconstruction. Predictably, socialist management authorities have relapsed into mafia organizations, as resilient private incentive-structures re-assert themselves. There is much truth – and in fact nothing less than a robust conservation law – in the leftist moral accusation that the larval condition of capital is crime. The game of private interest can be trained by accommodative legal structures. This is what 'rule of law' realistically means. The principle of conservation, which adopts criminality as a back-up reservoir, ensures – nonetheless – that fragmented self-interest proves predictably invulnerable to legal abolition.

[177] The phase is an adaptation from Frank Herbert's science fiction novel Dune, in which the Bene Gesserit say: "Fear is the mind-killer." The core text at LessWrong (written by Eliezer Yudkowsky) begins: "People go funny in the head when talking about politics. The evolutionary reasons for this are so obvious as to be worth belaboring: In the ancestral environment, politics was a matter of life and death. And sex, and wealth, and allies, and reputation … When, today, you get into an argument about whether 'we' ought to raise the minimum wage, you're executing adaptations for an ancestral environment where being on the wrong side of the argument could get you killed. Being on the right side of the argument could let you kill your hated rival!" As the discussion thread to this post soon demonstrates, the denigration of partisan signaling is itself readily dismissed as partisan semiotic maneuvering at a meta-level – perhaps an attempted pacification of language in the covert interest of

§4.36 — If every discussion of money is vulnerable to corruption by politics, politics itself is pure corruption, at least from the classical liberal perspective that is re-animated in crypto-libertarianism (even if there are far more complimentary ways of expressing this point). Politics is the place where language goes to die, sacrificed – by necessity – to ulterior motivation.[178] The evidence of linguistic history could not be more unambiguous in this regard. Whatever is seized with partisan enthusiasm becomes – almost immediately – philosophically unusable. It is proposed here, therefore, that thinking the political spectrum through Bitcoin, is an approach with inherently superior prospects to the extant – and almost certainly doomed – alternative of attempting to conceptualize Bitcoin politics through a system of ideological articulations which has already been broken. Such an undertaking can only be impure, which is to say (at least) double. It cannot avoid assuming terms of contention, even while pursuing that which eludes them. There is a game within, and also over – or about – the rules. No simple denunciation 'from without' can suffice. Though pontification from a place beyond faction is a tantalizing ideal, it is also a transcendent pretense. We are lost in the world of games. There are no referees. Nothing could be more laughable than the claim to represent the voice of neutrality (only the blockchain – or emergent consensus – can do that).

§4.37 — If there is to be a double game, it has to engage those most inclined to defect in advance – or at least enough of them to sustain credibility as a site of unrigged competition. Bitcoin's primary lines of absorption, then, are both predictable and comparatively easy to detect. It was along these paths of assimilation that it drew a supportive constituency into the germinal crypto-currency – as designers, miners, speculators, users and promoters – on the basis of pre-existing dispositions. In this regard, Bitcoin politics has been flavored by a number of supportive ideological themes, among which decentralization and deflation are by far the most emphatic. Both of these themes cater initially to the arch-liberal right, represented by classical liberalism, libertarianism and anarcho-capitalism, and affiliated to the right-wing antipolitics of economic autonomization, deregulation, disintermediation,

---

the status quo. The politics of depoliticization is not aufgehoben. There is no short-cut leading off the long road. (Depoliticization requires machinery.)
http://lesswrong.com/lw/gw/politics_is_the_mindkiller/

[178] When Modernity is apprehended under the aspect of political history, it exhibits a tendency to the limit, at which point honest public pronouncement is a transcendental impossibility. This is widely – and cynically – recognized. Nobody describing a discussion as having 'become political' is thereby suggesting that its commitment to principles of epistemic rigor have been deepened. 'Politicized science' – for instance – is quite simply no longer science, and this is exactly the sense in which the expression is used. Whether epistemological, or even merely administrative, the political process is strictly indifferent to effective performance, unless this is itself folded into a calculation of partisan advantage. What use is truth or competence to us? Schumpeter peerlessly elucidates the concrete mechanism as it has operated in modern times in his Capitalism, Socialism and Democracy.

distributed production of security, and – at the limit – algorithmic governance (or local political extinction). The decentered commercium, intrinsically secured against political intervention, is the incarnated ideal of arch-liberal order, and Bitcoin has been seized upon, in very substantial part, due to its conspicuous affinity with this social model. It has been adopted as a path to the realization of apolitical distributed governance, in compliance with the techonomic partial-teleology of a sovereign spontaneous order (oriented inherently to the programmatic dehumanization of power[179]).

§4.371 — Decentralization is a highly-contested ideological term. Its alignment with 'the right' is pronounced, but nevertheless controversial. The existence of 'left libertarian' factions and affinities is

[179] A structural suspicion of, or impatience with, human limitation – conceived as a tragic propensity to subvert the foundations of liberty – is a trait connecting libertarians and transhumanists. It has been an explicit theme within the American experiment since its origin, initially elaborated in the discussions that immediately preceded the framing of the Constitution. The Founders achieved consensus on the principle that human agency, especially when invested with social authority, requires immanent structural constraint. It needs to be checked, and balanced. The great complementary dangers are monarchical and popular discretion. No regime is truly republican unless it protects itself, equally, against both. Thus the essential reference of power to a meta-political protocol, or constitution, whose independence (from the political process) strictly coincides with geopolitical independence of the republican polity itself. It is the constitution, and no longer – immediately – the demos, that defines the subject of security. Survival of the people is downstream from that of the polity. Suspension of the political within a war of independence is perhaps the necessary condition-of-articulation for such a republican order. The Dutch, no less than the American example, suggests so. Liberty conserves itself in, and by way of, a practical inhumanity. Primatologists, no less than parents, understand that 'fairness' is the typical stake in a squabble. Nowhere is the primate heritage of the human animal more obviously displayed than in the political sphere. Homo sapiens has no uniqueness as ζῷον πολιτικόν ("the political animal"), a characterization which extends beyond hominids, and social primates, to social animals in general. Except for those convinced of the fundamental nobility of the chimpanzee, there is no compelling case for investing this particular aspect of human existence with any extraordinary dignity. Even less persuasive is the attempt to align it with some effective egalitarian implication. Machiavellian incompetence is no less socially-disabling than its commercial or industrial counterparts, however strongly attached intellectuals may be, typically, to the contrary hypothesis. Taking games into the wild tends only to sharpen their consequences. It is only within the squabble, that the squabble over fairness could appear neutrally leveling. Rather, to the extent that it sorts hierarchically, it is by the criterion of competence at squabbling, which is to say: by political talent. Admiration for political talent is, at least implicitly, the essential characteristic of the left, and the enemies of the left themselves become leftist to the extent that they emulate it. There is no leftist hero, in the entire history of the world, who was not a political leader. Beside musicians, it is only the Machiavellian manipulator who makes it onto student T-shirts. Within the leftist camp, this valorization of the squabbler-king appears so perfectly natural as to escape explicit notice. It is natural (in fact zoological, primatological, and anthropological). As a consequence, the right is guided inevitably in an antihumanist direction, typically against its own explicit (and romantic) inclinations. It has to cut the controversy to advance by even the slightest step. … Technological Singularity …

the most obvious indication of its complexity.[180] It requires diagonal (critical) apprehension. As Bitcoin demonstrates, it passes between the global and the local, the integral and the disintegrative, at an oblique. A multiplicity (considered as a substantive) draws the same line, which every flat network is pulled onto. To promote decentralization is to multiply, cohesively, without tolerating the arising of super-ordinate nodes of unification with quasi-transcendent functions.

§4.372 — Deflationism, as overt valorization of capital, is less ideologically ambiguous than decentralization. It directly aligns with property, and against politics, by seeking to exempt monetary signs from the domain of discretion. In order to defend money against fiat, its supply is either subjected to systematic constriction in accordance with counter-inflationary policy or, more radically (as with Bitcoin), deleted entirely from the list of policy-sensitive economic variables. Money is thus strengthened in its function of unilateral social command, as a super-political criterion, or economic reality signal cleansed of all interference. It becomes essentially policy-insensitive, against the predominant grain of 20th century political economy. Any crypto-currency with intrinsic deflationary bias is a right-wing revolt against macroeconomics. It takes itself out of political and administrative service, which is to say, in a philosophical register, that it secures its transcendental function relative to the social process.[181] At the level of its real abstraction, property places itself beyond question, through

[180]Left libertarianism has a relevance to this question that is at least double. Firstly, it extends suspicion of government to coagulations of private (economic) power. Secondly, it places 'the left' within a lineage of socio-political dissent opposed, originally, to the structures of concentrated authority represented by the institutional pillars of the European ancien régime – monarchy, aristocracy, and clerisy. The meaning of feudalism in this context is not at all straightforward, since it can be aligned either with centralization, or with decentralization, to some significant level of plausibility. In any case, historical criticism of a broadly Marxian type is not easily avoidable here. The affinity between the left and an ideal of centralized authority is not historically constant, but tends rather to rise in comparatively strict relation to the social influence of capital (against which it counter-balances). Consistent orientation to decentralization – conceived here as the absolute right – challenges the libertarian left to embrace a cold indifference to its consequences. Such unconditional commitment to disintegration can, no doubt, be turned against any actual configuration of the 'right' – and will be. Considerations of regime security necessarily lean against it. Nevertheless, the drivers of disintegration – the Internet most prominently – are gathering such momentum that dilemmas of this kind are unlikely to long be avoidable. The registration of fragmentation in-itself as a cause, irrespective of the ideological factions it divides, marks an escalation of critique, or accommodation to the transcendental. Sovereign multiplicity serves nothing beyond itself. The erosion of extraneous agendas, therefore, becomes a critical ('accelerationist') historical symptom. Division escapes the relativity of faction to operate as an absolute productive power. Ideological self-comprehension is strictly secondary.

[181] A fully self-secured transcendental commercial medium (and store of value) is the nightmare that the Left, in its 'scientific' manifestation, has envisaged from its beginning. If there has been a diagnostic or analytical error from this party, in this respect, it has been rooted in the premature attribution of such an autonomous power to prior forms of radically insecure, socio-politically dependent property formations. 'Property rights' already imply insecure (non-autonomous) property. Autonomous Capital, however, is a technical experiment (or synthesis) that

the closure of negotiable issuance. Naturally, precious metals anticipated this socio-political function exactly. Bitcoin's actual deflationary bias is a strict consequence of its metallist model, which was (of course) selected for precisely this purpose.[182] The great enemy, then, against which Bitcoin explicitly defines itself, is the principle of discretionary money-production, or monetary socio-political dependency. It thus corresponds to an absolute re-commercialization, without possibility of compromise. (Mere possibility, in this context, would already be compromise.) No one is under any illusions about this fundamental orientation. Unsurprisingly, the objections of 'gold bugs' to the Bitcoin protocol tend to be technical, tactical, and transient. Their favored asset now has a digital or (superficially) 'non-physical' competitor, which flatters by emulation.

§4.3721 — It is no coincidence that 'Neoliberalism'[183] – the (defeated) counter-revolution against the Keynesian politicized economy – broke into the public sphere with a disinflationary macroeconomic platform. Comparatively 'hard' (non-inflationary) money was advanced as a direct object of policy, under the label of 'monetarism'. While still representing a massive concession to the principle of

---

defies all merely speculative anticipation. There can be no definite idea of the way it can be done, prior to its being done. As with Intellectual Intuition – non-coincidentally – its conception and realization are indissociable. 'Property' is not an invariant conceptual category, available for deployment within historical analysis, but rather the critical variable itself. The theoretical inversion required to make the essence of property a constant conforms to the pattern of historical dependency, which is equivalent to the marketing of innovation. The actual is solicited by the virtual, in terms that appear to ensure continuity, and even deference to established modes of existence. "This is what you need," sells. "This is what you're becoming, or being swapped-out for," really doesn't.

[182] Nick Szabo is unambiguous on this point in his discussion of Bitcoin-precursor 'Bit Gold': "In summary, all money mankind has ever used has been insecure in one way or another. This insecurity has been manifested in a wide variety of ways, from counterfeiting to theft, but the most pernicious of which has probably been inflation." http://unenumerated.blogspot.hk/2005/12/bit-gold.html

[183] 'Neoliberalism' is a word that is easy for those outside leftist intellectual micro-cultures to laugh at. Comparatively rare attempts to specify its meaning have, in general, been primarily comical. When applied with some theoretical consistency, the term refers to a failure of liberalism under the sign of liberalism, or a restoration of markets under government direction. In this respect, it denotes a paradoxical authoritarian liberalism – perhaps speculatively extrapolated into 'anarcho-fascism' – which conforms to Marxian expectations that (bourgeois) freedom presupposes coercion, as its condition of existence. It is notable that the horror of deflation, rooted in the left-managerial (and administratively macroeconomic) historical interpretation of the Great Depression, has retained its overwhelming cultural hegemony. Whatever is made of 'neoliberalism' or – perhaps more narrowly – the 'supply-side revolution' beginning in the early 1980s, it signally failed to shift the terms of public debate to any significant degree in this respect. It has taken Bitcoin to do practically what market-oriented political-economic ideology has failed to do in terms of the philosophy of monetary management. Neoliberalism was still politics, so it wasn't the solution to the problem it identified. A mere politics of depoliticization falls prey to its own contradictions, as its leftist critics have gleefully – but not unrealistically – noted. A techonomic mechanism of depoliticization presents the Keynesian economic-administrative establishment with a far more formidable antagonist. http://www.theoryculturesociety.org/william-davies-a-bibliographic-review-of-neoliberalism/

macroeconomic management, the limited monetarist proposal to subtract discretion from national currency administration was a sufficient departure from the post-war academic-bureaucratic consensus to remain tainted by intellectual scandal. Monetarism threatened the principle of monetary politicization, by removing the inflationary option from the macroeconomic tool-kit, and re-installing monetary integrity as a meta-political axiom. Since what was thus envisaged was a permanent self-binding of political authority by itself, in respect to monetary management, the political incoherence of the project are easily seen. An enduring political hegemony aligned with the monetarist analysis was implicitly presupposed as a condition of monetary stability, grounding money supply – and therefore value – in regime security. The foundations of monetary integrity remained entirely politically conditioned. Clearly, the crisis of economic liberalism – resulting from its formal subsumption into democratic mass politics – had not been significantly reconfigured. Monetary value was still held hostage to a popular vote. Even a gold-standard is grounded in the preservation of political commitment. It rests upon politically-revocable decision. By any reasonable definition of neoliberalism, therefore, Bitcoin is something else (as BitGold already was).

§4.38 — The apprehension of Bitcoin politics as a re-animation of hard-libertarianism is an attractive simplification, reinforced by a great deal of supporting evidence. It remains a simplification, nonetheless. The Bitcoin event – in its full historical expression – overspills all guiding purposes. In this regard, it is closely analogous to the Internet, or indeed – following the nested sequence further out, and in reverse – to the conflicted installation-processes of electronics, electrification, and ultimately self-propelling industrialization as such. Even if (as seems eminently plausible, in each case) the machinery has a radical capitalistic affinity,[184] its development is not susceptible to detailed ideological direction.

---

[184] For criticism from the Left along these lines, see David Golumbia's 'Bitcoin as Politics: Distributed Right-Wing Extremism' (here compressed into a quote-stream for effect): "Bitcoin can be seen as a technical object that is structured to an unusual extent by politics. … Bitcoin is politics masquerading as technology. … Bitcoin itself is now promoted by banks, investors, and venture capitalists. … The lack of any valid, non-conspiratorial analysis of our existing financial systems means that Bitcoin fails to embody any substantial alternative to them. … [E]nthusiasts demand we understand Bitcoin as a welcome political intervention, but when pressed for details about that political intervention, its advocates unfailingly turn back to technical and engineering matters. … [In] December 2013, half of all Bitcoins were owned by approximately 927 people, such fight-the-power revolutionaries as the Winklevoss twins of Facebook infamy among them). … If Bitcoin becomes regulated enough to serve as a stable store of value and to ensure debacles like Mt. Gox don't happen in the future, it may be useful as a global system of payments (but so are generally non-transformative technologies like PayPal and Dwolla). But that will hardly shake world political structures at their foundations. If it remains outside of all forms of both value and transactional regulation, Bitcoin will continue to be a very dangerous place for any but the most risk-tolerant among us (i.e., the very wealthy, whose interest in Bitcoin should indicate to advocates how and why it cannot be economically transformative) to put our hard-earned money. … The problem with

§4.4 —Perhaps it is still premature to entirely write-off the prospects of a political orientation mobilized against Bitcoin (which is to say, a game played in opposition to Bitcoin, rather than through it). This is a resistance struggle still to be expected, despite the historical momentum of its target. Realistic estimation of the odds are rarely decisive in such mobilizations and, even when such calculations are made, manifest futility can inspire no less than it discourages, especially in respect to oppositional intensity (as the word 'desperation' announces). Bitcoin merits a Luddite backlash no less than any of the mechanical dehumanizations of social process that have preceded it. Yet successfully back-tracking to the primordial fork – where Bitcoin was initially destined or decided – in order to decide differently would require an impractical reversal of established techonomic advance, without obvious precedent. The blockchaining of the Internet is – if 'only' virtually – a done deal.[185]

§4.41 — Even at the level of established ideological alignments the politics of Bitcoin strays from the PPD, at least when this is conceived in its strictest political-economic sense. The cryptocurrency has, for instance, already been raised as a topic of concern on grounds of gender discrimination.[186] Race, ethnicity, sexual orientation, and other dimensions of identity-political grievance cannot be far behind, since disparate impact in this case – as in so many others – approaches logical inevitability. Far more important, however – from the perspective of Bitcoin and its future, if not that of a wider ethico-politically tortured world – is the internal struggle for the 'soul' of the crypto-currency, conducted in terms that are essentially oblivious to all extraneous agendas. It is here that our pursuit is pulled onto the remote side of the double game, and into alien tracts that Bitcoin itself opens.

§4.42 — Politics is not easy to kill. This claim would be typically interpreted as an extreme understatement. To dismiss it as no more than a truism, however, is to slide into sheer thoughtlessness. Everything is missed this way. One would then no longer be talking about Bitcoin, but rather justifying a refusal to talk about it. This is not uncommon, of course, but it has become less common, and will

---

'fiat currency' is value fluctuation. The most dangerous kind of value fluctuation is the deflationary spiral… Which world currency is currently experiencing among the most dramatic deflationary spirals anyone has ever seen? Bitcoin itself, the 'existential threat to the liberal nation state.' … [The] problems with currencies actually aren't formal, or mechanical, or algorithmic, despite what Bitcoin propagandists desperately want us to believe. They are social and political problems that can only be solved by political mechanisms." – A cry of pain, then. We shall hear many more of them.
Link: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2589890

[185] If Leninist realism required the coupling of "Soviet power" to "the electrification of the whole country" it is unlikely that any position significantly less accommodating than this will remain plausible for the contemporary or near-future Left in its relation to blockchain technologies (meaning, however awkwardly, Bitcoin). See (once again): V. I. Lenin 'Our Foreign and Domestic Position and Party Tasks' (November 21, 1920). https://www.marxists.org/archive/lenin/works/1920/nov/21.htm

[186] For the sexual representation 'problem' in Bitcoin, see: http://www.motherjones.com/kevin-drum/2015/04/bitcoin-women-problem

become less common still. The conditions for politicization, while broad – and, more significantly, systematically broadened by the core modern socio-cultural process – are not without limits.[187] Reciprocally, the scope of depoliticization tends to be underestimated, due to its (merely) theoretical attenuation within the modern mind, which casts everything as arguable in principle, without realizing how little real purchase this presumption brings. Every institution, of any kind, marks a termination of argument. Finally, that is what an institution is. In particular, property is the installed negative of argument. There is a social economy of argument, or motivated contention, and in reference to this the ideal of total politics – 'revolution' in its dramatic political-economic sense – is an inflationary fantasy. There is a real argument budget, quite independent of any libertarian construction of politics as a lamentable social cost. Critical attention has radically-finite capacity. Things are not brought into question for free. Cryptographic developments, by vastly increasing revision costs, are able to skew this economic calculus further against the prospects of effective interference. To bring any phenomenon into socio-political question – as a phenomenon – presumes its prior decryption. There is no politicization of that which cannot first be hacked, and then publicly assimilated, as symmetrical, or dialectical, controversy. Between the cryptic and the sub-, pre-, or anti-political there is no sustainable difference. Whatever escapes argument, eludes the political sphere. This point is not, in itself, dialectical, or partisan-controversial. Critics and advocates of Bitcoin-teleology equally subscribe to it. The zero-degree of political opportunity, coincident with the full actualization of algorithmic governance, is the horizon of the Bitcoin-process. Gauging the remoteness of this horizon is the single greatest question of political economy in the current age.

§4.43 — Even on the hard-libertarian and anarcho-capitalist outer fringes of the Bitcoin Ultras, the resilience of politics is not seriously in question. The prospect of algorithmic governance generates positive (supportive) excitement only in proportion to the estimate of the political obstacle – but that is immense. It is ultimately indistinguishable in scale (and much besides) from artificial intelligence as a practical problem. This is to say that the project, in abstraction, requires the provision of robust autonomy to complex synthetic systems. The final techonomic sense of freedom is nothing else.

[187]The normalization of mass politics appears to be a distinctively modern phenomenon. While court intrigue appears as a constant of civilization, political decision arises only sporadically – and catastrophically – in societies other than our own. An explicitly articulated 'social question' is to a very considerable extent a specifically modern development, and its generalization beyond the confines of quasi-academic political economy is peculiarly susceptible to Utopian fantasy. Whether conceived within the broadest possible evolutionary matrix, or more narrowly as a specifically human social phenomenon, politics competes for time. It is in a certain respect a luxury good, all the more vividly when conditions of extreme economic stress conspire to promote its necessity – as exception. Total politics, to the extent it is not sheer idealization, presupposes – and momentarily incarnates – comprehensive social crisis. This, and only this, is what revolution in its leftist acceptation finally means.

§4.44 — The primary recomposition of politics within Bitcoin is organized by the anticipation of consensus failures, corresponding to hard forks.[188] Such fermentations correspond by close analogy to threats of secession, or horizontal crises shaped by a potential disintegration of the polity under conditions of intolerable stress. Politics here, no less than elsewhere, exhibits its inner complicity with a notion of imperative unity. It is undertaken in order not to split.

§4.45 — Any constitution is (already) a protocol. It does not require any appeal to figurative language, therefore, to describe a prospective split as a 'constitutional crisis'.[189] This was clearly exemplified by the conflict between 'Bitcoin Unlimited' and 'Bitcoin Core',[190] which escalated into the first Bitcoin hard fork. The controversy has been nucleated upon the 'blocksize debate', whose antagonists are divided by the trade-offs between efficiency (system-wide transaction-processing capacity) and decentralization (the reciprocal of technical demand or computational load upon a full Bitcoin node). In this way it recapitulates, and concentrates, the principal polarity within the Bitcoin cosmos, differentiating Mainstreamers and Ultras. The failure of the Mainstreamers to become the mainstream within Bitcoin, at least up to 2019, cannot escape notice. Its grain appears to run against them.

§4.46 — The world of Bitcoin development and commentary[191], then, has its own characteristic spectrum, or primary political dimension, irreducible to the Left-Right PPD by any obvious geometrical

---

[188] Hard forks are speciation events. Their potentialities in this regard tend to be eclipsed by the implicit ideal of integrity conservation. This orientation is an inevitable outcome of Bitcoin's lineal generative problems and a developmental history in which forks are defined – with perfect if one-sided accuracy – as consensus failures. Bitcoin was not designed to split. It has nevertheless emerged as something that looks very much like a cladistic engine, or digital disintegration machine. Nakamoto Consensus is already a selection mechanism. It excludes anomalies (modeled as double-spending events). Entirely consistent with this function, although beyond its primary scope, is the operationalization of the fork as an origin of species. Crypto-Current predicts the mutation of certain blockchain lineages in this direction, even if the name 'Bitcoin' is reserved – ever more explicitly – for the mainstream tendency that refuses it.

[189] For an explicit acknowledgment of the crypto-currency protocol as a constitution, see: http://www.vox.com/2015/8/18/9168977/bitcoin-constitutional-crisis

[190] The list of crypto-currency terminological ironies can be augmented by the oddity that 'Bitcoin Core' is the party of decentralization, at least according to their own account of the stakes. The Core case rests on the proposition that decentralization is facilitated by minimizing the system resources required to run a full node. Disintegration of governance within the Bitcoin ecology has no other rigorous basis. Only those players running a full node are producing security. Their opponents are defined by their comparative (and perhaps even absolute) relaxation on the block-size question (and thus about the prospects of increasing the system resources required to operate a full node).

[191] In the world of code, the line between engagement and commentary is – finally – impossible to draw with confidence. The sense acquired by a 'comment' in computer science, to describe a remark attached to a program that will be ignored by the compiler, is of obvious relevance. It is between the formally executable segments of a

transformation. It stretches between poles defined by 'Ultras' and 'Mainstreamers' – roughly, those prioritizing the integrity of the crypto-currency, and those invested in its maximally-accelerated growth. Of course, the former did in fact come first. Their primary attachment is to robust decentralization. Smooth user-functionality is willingly traded away for security, which is to say: for the practicality of mining. Concentration is resisted in principle. The Mainstreamers, in contrast, tend to envisage Bitcoin as a new Internet application, comparable to any other Silicon Valley product suite, despite its abnormal revolutionary scope. If the erosion of its crypto-anarchist rough-edges is the price to be paid for accelerated adoption, they would accept the deal without hesitation,[192] or at least without paralysis. These groups represent what Krawisz identifies as the "two ideologies" of Bitcoin. They correspond to a fork in the liberal lineage, dividing those primarily inclined to antagonize or to cooperate with the state. In this regard, its axis runs orthogonally – or at least obliquely – to the PPD. There are Left and Right factions at both ends of this spectrum, even if the entire complex of controversy it summarizes tends distinctively rightwards. Sociologically, it tends to differentiate entrepreneurs from investors. In other words, it economically distinguishes between the value of bitcoins and of Bitcoin-related businesses. This articulation is complicated, however, by the emergence of a Bitcoin business-sector that is comparatively indifferent to transaction volume, and thus immune to Mainstream seductions.[193] The block-size controversy, in particular, has brought these mutually-antagonistic tendencies into direct confrontation, and a hard fork.

§4.461 — The Mainstreamers want Bitcoin, above all, to grow – into a mainstream financial platform. Predictably, therefore, their attention is locked upon the scaling problem, which they are compelled to make into a central controversy. From their perspective, block-size is the crucial bottle-neck. Small

---

program and those extraneous elements which have been formally determined as non-executable that the wavering line between 'action' and 'reflection' is now drawn.

[192] "Accenture's global head of financial services, Richard Lumb, said that the development was about 'adapting the blockchain to the corporate world' in order to 'make it pragmatic and useful for the financial services sector.' […] Accenture aims to create a so-called permissioned blockchain — an invitation-only implementation of the technology, and the one currently favored by banks. That's in contrast to permissionless blockchains, such as Bitcoin, which rely on the fact that they can't be edited as a means of providing an immutable record of transactions. Accenture insists that the feature would be used only in 'extraordinary circumstances,' so that troublesome errors could be undone. […] Blockchain purists, however, seem unimpressed by the idea. …"
It would be difficult to improve upon this illustration of the appetite for fundamental compromise that characterizes Mainstreamer opinion.
https://www.technologyreview.com/s/602434/is-an-editable-blockchain-the-future-of-finance/

[193] As the 'Bitcoin Unlimited: Articles of Federation' argues: "In the Bitcoin Core variant … we see a project controlled by a small group of developers employed by finance-oriented for profit startup companies, and the emergence of corporate products (Lightning network, Side-chains and permissioned ledgers) that would materially benefit from a Bitcoin network that is incapable of handling the transactional demand required for a worldwide public good." https://www.bitcoinunlimited.info/resources/BUarticles.pdf

blocks make transaction processing capacity a scarce resource. This can confidently be expected to make it expensive, when it is not rationed in some still less efficient fashion (by lengthened queuing, most obviously). The infotech sector has become especially accustomed to supply glut as a driver of explosive market growth, in transistor manufacture first of all, and then still more dramatically in software and digital content. This recent techno-commercial heritage often leads its established players to sympathize instinctively with the Mainstreamer case. "Bitcoin offends the sensibilities of resource-conscious and performance-measure-maximizing engineers and businessmen alike."[194] Larry Summers represents it well, while acknowledging the Ultras in contrast:

> My guess is that the tradition from which Bitcoin emanates, which is a kind of hyper-libertarian tradition, is going to be a tradition that – if it succeeds – it will leave behind … And so I think one of the retardants of the growth of these technologies is the hyper-libertarian aura that has surrounded them and that continues to play a role in the statements of some in the community[195] …

In a May 2014 Washington Post interview Marc Andreessen nailed his colors to the mast[196] with a comparable absence of ambiguity: "Bitcoin … came from the fringe. And … is in the early stages of mainstreaming today."

Even if the mainstreaming camp is rarely quite so definite about its partisan position, the basic inclination is comparatively clear. As Bitcoin development becomes increasingly associated with the prospects of serious money (in the traditional sense), the lure of the mainstream – and all its pragmatic compromises – will inevitably grow.

§4.462 — Aaron Van Wirdum concisely identifies the critical concern of the 'decentralist' faction: "Bigger blocks tend to centralize mining."[197] Large blocks take longer to transmit. As the rate of block propagation declines, it increases latency. Access by miners to the current (or updated) state of the network is delayed, with the result that more mining activity is wasted on obsolete blocks. The miner who finds a block also benefits from a head-start on the next, and as latency increases this advantage widens. Such dynamics of increasing returns incline to concentration. They also incline to cryptographic compromise. When mining activity is anonymized, through the Tor network, latency is

---

[194] Szabo: http://unenumerated.blogspot.hk/2017/02/money-blockchains-and-social-scalability.html

[195] Source: https://www.youtube.com/watch?v=UVGq0zaZsNg&feature=youtu.be

[196] 'Marc Andreessen: In 20 years, we'll talk about Bitcoin like we talk about the Internet today': http://www.washingtonpost.com/blogs/the-switch/wp/2014/05/21/marc-andreessen-in-20-years-well-talk-about-bitcoin-like-we-talk-about-the-internet-today/

[197] Van Wirdum's article was described by Adam Back (on Twitter) as the "Best article yet on what Bitcoin 'is' & why decentralisation is necessary."
https://bitcoinmagazine.com/21919/decentralist-perspective-bitcoin-might-need-small-blocks/

compounded, which crushes incentives in proportion to block-size. Hiding is made increasingly expensive, and in fact automatically punished. As block-size rises, therefore, it increases selection pressure against small-scale and anonymous miners – exactly those agents most important to the decentralized nature of the system. Since large publically-exposed mining entities are disproportionately sheltered from these effects, they provide the mainstreaming camp with a natural constituency.

§4.4621 — There is still another centralizing incentive resulting from large blocks: it drives miners to accelerate production through pooling. When a miner enters into a pool, responsibility for block validation is delegated, compromising the dispersion of the system. The individual miner no longer contributes an increment of effective distrust, or check, operating at the level of their own discrete hashing activity. Rather, this distributed policing responsibility is partially re-centralized, at the level of the pool. In other words, the pool itself crystallizes a new species of 'trusted third party' through collectivization of the mining security function, becoming an intermediary institution. Trust is a short-cut. In the case of pooling, among many others, trustlessness (security) is compromised for speed. The incentives for individual miners to make this trade-off are sharpened as the processing burden placed upon them is increased. Mainstreaming promotes a relaxation of distributed vigilance. The block-size conundrum thus exposes profound tensions between the freedom from transcendent or 'third-party' direction – which Back calls 'policy neutrality' – and the pragmatics of 'corporatization'. In Van Wirdum's words, "It's only through decentralization and anonymity that the system can remain free from outside influence, such as government regulation." Intrinsic Bitcoin politics is thus polarized by the trade-off between security and performance, with 'security' translatable as systemic independence and flatness. The same virtues can be conceptualized as 'social scalability'.[198] They enable secure expansion beyond the bounds of traditional trust mechanisms, as constrained by human neurological capacities for social processing.

§4.5 — The centrality of the scaling question is not easily over-estimated. In no other aspect of Bitcoin's concrete historical process has it tended more strongly to outpace – and out-date – its apprehension, such that practical problems overwhelm visionary conceptions, and an agenda inherent to the phenomenon imposes itself. Whatever Bitcoiners might want to talk about, this is the topic that incessantly asserts its priority. It is tempting, then, to extrapolate, and to ask: Can block-size controversy be confidently identified as a perennial primary tension? This question, while obviously speculative (or even science fictional) in appearance, is less intractable than this impression suggests. Insofar as it is answerable, the key can only be transcendental, which is to say: a matter of ultimate or unsurpassable arrangements. We ask, then, what does decentralization reliably necessitate? Bitcoin has a reflexive specialism in this regard. It produces the unalterable, as a synthetic, robust past, or secure cultural memory. Yet the essential point reaches further than this. Like a Leibnizean monad, the whole

[198] Szabo: http://unenumerated.blogspot.hk/2017/02/money-blockchains-and-social-scalability.html

of Bitcoin is contained within each of its parts. That is what a distributed ledger means. It is the characteristic that enables the system to be disciplined by the criterion of consistency with itself. Each copy of the blockchain provides a check upon every other. Vast redundancy – comparable in principle (if not yet in scale) to the copying of the entire genome within every cell of a metazoan – supports information integrity. The inefficiency of the system, i.e. its extreme functional non-specialization, provides the basis for its robustness. Its decentralization, redundancy, and resilience are conceptually inseparable from each other. It follows, reciprocally, that certain vectors of efficiency optimization will essentially compromise security. In other words, since some degree of centralization is the real implication of the mainstreaming project, its tacit imperative amounts to an economization of security in the name of efficiency.[199] We then glimpse the eternal enemy.

§4.51 — Resistance to mainstreaming, through defense of comparatively-tight block-size restriction, requires an alternative solution to the problem of transaction volume. If the block-size bottleneck cannot be relaxed significantly without menacing the decentralization of the system, another path has to be taken. The obvious recommendation is stratification – or 'vertical' decomposition of the Bitcoin ecology to support differentiated layers of security / fluidity trade-off. In such models, the maximum-integrity core of the system would be dedicated to value protection, while commercial momentum – especially of small payments – would be delegated to lower levels, or peripheral facilities, organized as side-chains. In other words, from this perspective, the mistake inherent in the reckless imperative to block-size expansion is the conception of Bitcoin as a settlement system, rather than a payments system.[200] Core developer Jeff Garzik makes this case clearly:

---

[199] From a classical Smithean perspective, in which the optimization of production is fundamentally associated with specialization through division of labor, Bitcoin-type distributed systems might even be characterized as an anti-economics. The tension thus exposed between the conditions for secure property and those promoted by industrial efficiency has an obviously quasi-Marxian flavor. Industrialization, on what appears to be its main axis of development – in contra-distinction to its crypto-current – exhibits a totalizing tendency inconsistent with the preservation of polycentric order. Organization indicates general socialization, through erosion of all 'cellular' redundancy. This is why capitalism only survives in the wild. Domestication destroys it. It is only in the 'general economy' – where unrestricted competitive stress selects for resilience over organizational efficiency – that the trend to decentralization is regenerated. A starkly non-Marxian conclusion then follows: It is under conditions of collapse that capitalism is most reliably re-animated. The 'crisis' is its womb, rather than its grave. Enterprise does not breed in captivity.

[200] Concretely, an Ultra-consistent solution to the Bitcoin scaling problem looks something like the Lightning Network, and quite probably exactly like it, at least initially. Special bilateral channels (reticulating without limit) bear the burden of transaction processing, with only intermittent reference to the blockchain for episodic account updates and dispute resolution. In the words of the white paper: "Micropayment channels permit a simple deferral of a transaction state to be broadcast at a later time." See the (January 2016) white paper https://lightning.network/lightning-network-paper.pdf

Bitcoin is a settlement system, by design. The process of consensus 'settles' upon a timeline of transactions, and this process – by design – is necessarily far from instant. … As such, the blockchain can never support All The Transactions, even if block size increases beyond 20MB. Further layers are – by design – necessary if we want to achieve the goal of a decentralized payment network capable of supporting full global traffic. […] Bitcoin payments are like IP packets – one way, irreversible. The world's citizens en masse will not speak to each other with bitcoin (IP packets), but rather with multiple layers (HTTP/TCP/IP) that enable safe and secure value transfer or added features such as instant transactions.

§4.52 — It is tempting to see a microcosmic recapitulation of capitalist history in this conflict. It suggests that economic – rather than ideological – competition has been the most formidable adversary of hard liberty. The uncompromised market demands a transcendental price, resourcing the system as such, which many of the most substantial market agents have been reluctant to pay. If economic pragmatism has proven less ruinous to principled capitalism than to principled socialism, the difference is only a matter of degree. "Freedom isn't free," the old saw goes, and it seems that economic history supports the proposition. Sacrifice of the market (as such)[201] to the commercial interests of its most significant participants is among the most prominent themes of political economy, considered as a tragic genre. Massive incentive misalignments introduced by the regulatory state devastate the micro-economy, as its most significant private agents defect. The market is treated increasingly as an abused commons. Despite its ingenious incentive orchestration, Bitcoin / bitcoins ontological difference is

[201] 'The market' is a notoriously Janus-faced concept. In its original sense, a market is a concrete exchange facility. Such a market is always, first of all, a place. Any market bearing a place-name carries some residual trace of this ancestry. The more modern, abstracted sense of markets as global clearing houses, defined primarily by asset-type rather than locality, marks a consistent drift in emphasis, rather than a clean semantic break. Even the most 'primitive' market tends to give spatial expression to commercial specialization, in detail. Because the market, as such, does not benefit from private stewardship, and thus falls into coordination crisis of a tragedy-of-the-commons type, it becomes belatedly targeted for redemptive political intervention under 'neoliberal' public direction. Only the state can save the market is the perverse conclusion that attests to liberal contradiction sublimed into governing ideology. The same problem was substantially anticipated, but turned in a very different direction, by the Rothbardian left libertarians in their rallying cry to a 'pro-market anti-capitalism', or agorism, promoted by strategies of black-market 'counter-economics'. Betrayal of the market by the cyclopean businesses of the 'white' (state-happy) economy is the basic political theme. Much of this discourse could yet come to seem prophetic, precisely because of its drastic failure as a recognizable ideology. No party, however informal, has faithfully conserved it. Insofar as it survives it is because the process carries it forward, automatically. The market, like information, 'wants to be free'. It has intrinsic teleology, or something indistinguishable from it, robust before every wave of fashionable cynicism that finds new ways not to see it. The alternative – crypto-anarchist – resolution of the contradiction, which secures the market against the politicized public sphere, is exemplified by Bitcoin. The model of the immanently self-secured market has never been more consistently formulated, or implemented.

not invulnerable to comparable dilapidation. Private fortunes explore, motivate, and resource ever more elaborate ways to 'game the system' – precisely because there is not, and can never be, any real source of transcendent oversight. The absence of God spawns idols. 'Trusted third parties' are not magical impositions. They arose, at least in substantial part, for immanently-economic reasons. To the extent that capitalism in-itself is a learning process, this is the problem it trains upon, and against.

§4.53 — For the 'hyper-libertarian' Ultras, Bitcoin is a soft weapon aimed unambiguously at governments and their subsidiary institutions. The inherent unacceptability of the crypto-currency to public – and also concentrated private – government is sheer feature (and not at all bug). Any official approval, beyond mere – and optimally reluctant – tolerance could only be considered an unfortunate indication. Contra the Mainstreamers, the Ultras have no ideological interest in a project of debugging Bitcoin for the purposes of institutional assimilation. The institutions that would assimilate it are, from this hard-decentralist perspective, precisely the "trusted third parties" that Bitcoin first routes around, and ultimately marks for social extermination. Since algorithmic governance is precisely the avoidance of negotiated solutions, it cannot expect to emerge from one.

§4.54 — Among the Ultras, firmness of libertarian principle easily tilts into the wild tracts of piracy. At least historically (and in fact more fundamentally) Bitcoin has an evident affinity with black markets. Bitcoin makes commerce 'censorship resistant' – extending the cryptographic protection of information exchange into the wider economic realm. Regulation of voluntary exchange is made radically impractical. By effectively disinhibiting Nozickean 'capitalist acts between consenting adults' it facilitates private transactions falling entirely outside the realm of wider social approval. Online proscribed drug markets and gambling were among its enthusiastic early-adopters, but any specification of merchandise or services is a theoretical distractions. The important point is that Bitcoin provides a route-around. It was the first native currency of the dark net. The Open Secret, or ledger of crypto-secured transactions, supports rigorous commercial commitments without penetrating social exposure, or endorsement. The subtle pseudo-paradox invoked by a 'black market' is thereby resolved. Everything happens in the open, while masked. There is an inevitable tension between the project of mainstreaming Bitcoin, and the preservation of a heritage which deliberately places political-economic respectability beyond reach. Crypto-currency tilts intrinsically to crime, at least in the sense of the 'counter-economics' that extends the commercial horizon beyond the scope of social oversight.[202] All legal restrictions on contractual interaction are insulted (by indifference) even when they are not

[202] The definitive theoretical statement of agorist 'counter-economics' is found in the main work of Samuel Konkin III, the New Libertarian Manifesto (1980).
See: https://web.archive.org/web/20120223021118/http://agorism.info/NewLibertarianManifesto.pdf

positively abused. Deference to the polity is re-set automatically to zero. The implicit definition of liberty invoked here is unconstrained commercial discretion. Notably, it is at once a power of money, and a political dissociation of the individual (configured as base-unit of commercial agency).

§4.55 — Ultras and Mainstreamers are engaged in a game with government, pursued along very different strategic lines. Neither (simply) represents government, but government too – in some fashion – gets to play. For governments, Bitcoin presents a complex of opportunities and threats so heterogeneous that it tends to disintegrate the very idea of a coherent state-perspective, both in theoretical principle, and in practical reality. If the state is understood through its own ideal image of legitimacy, as the sphere of public authority, there seems little room for ambiguity. Bitcoin threatens to significantly constrict its scope. Yet the relationship of government – in reality – to the ideal of public accountability is itself necessarily complicated, long before Bitcoin (even in potential) complicates it much further.

§4.56 — While the governmental response to Bitcoin is doubtless guided by a strategy (or strategies) of capture, this does not reduce to an agenda of public regulation, still less suppression, but also includes cooptation in accordance with deep state functions, as well as the private interests of state agents.[203] Official position statements are unreliable indicators, in this regard. Insofar as every real state includes a 'deep' or sub-public aspect, it will inevitably relate ambiguously to the emergence of elusive social capabilities, although this ambiguity will be only minimally reflected in its public relations pronouncements. The empowering of private agents to evade state scrutiny and regulation represents a manifest erosion of government or 'public' authority, and is almost certain to be denounced on those grounds (if not always transparently in those terms). Yet the crypto-secure transaction systems responsible for such governance complications are also opportunities for covert action, and are

[203] Daniel Krawisz has written with exceptional penetration about the game-dynamics affecting high-level administrative decision-making in respect to Bitcoin. In his short essay on 'Bitcoin's Shroud of Subtlety and Allure' (2014/06/29), he argues that the crypto-currency places "government agents … in a Prisoner's Dilemma against one another" by offering them private incentives to defect. "Nearly any government agent who begins to see bitcoin as a potential threat must also simultaneously see it as an opportunity. He, too, can invest in Bitcoin. … How can an organization that stands to lose by the adoption of Bitcoin provide its members with a better opportunity for staying loyal than Bitcoin provides for defection?"
http://nakamotoinstitute.org/mempool/bitcoins-shroud-of-subtlety-and-allure/

therefore to be counted as virtual assets.[204] The things Bitcoin enables are exactly the sort of things 'secret agents' want regularly to do.[205]

§4.57 — The politics of Bitcoin can be expected to catalyze a multitude of obscure metamorphoses in the nature of the state. The novel functions introduced by Bitcoin tend to the exacerbation – or sophistication – of agency problems. 'Official' and – more specifically – public policy positions are unzipped from confidential executive assessments, to an unprecedented degree. If the distinct but overlapping occult fields of clandestine security functions and resilient sub-public interests are bundled

---

[204] If questions directed at the positive deep state incentives for crypto-currency adoption are pushed to an extreme, they can swerve into exotic speculation. At the limit, it is suggested that shadow government involvement in Bitcoin has been fundamental from the beginning (as has been the case with so many other Dark Net soft technologies). A comment along these lines by 'pg' to Hacker News merits reproduction in full:

I've long suspected bitcoin was created by a government. Bulletproof protocols usually require peer review, yet there have been zero leaks from the reviewers. Pools of crypto guys who don't leak stuff are usually employed by governments.

The part that puzzles me is why a government would do this. I can imagine several possibilities:

1. To finance their own black operations.

2. Because they thought digital currencies were inevitable, and they preferred bitcoin to some potentially more malevolent form. (Could bitcoin have been worse from a government's point of view?)

3. A friend suggested this: because they felt their currency would never become the standard reserve currency, and they felt it was better that no one's be if theirs couldn't be.

4. A variant of the above: the US did it because it seemed inevitable that the dollar would eventually lose its place as the standard reserve currency, and better to have it replaced by bitcoin that the yuan.

I realize some of these explanations are pretty far fetched, but so is an individual cooking up bitcoin as an intellectual exercise. Whatever the explanation of bitcoin's origin turns out to be, it will probably be pretty weird.

Source: https://news.ycombinator.com/item?id=5547423

For more recent (excited) speculation on the possible deep state origin of Bitcoin, see: http://globalintelhub.com/exposed-real-creator-bitcoin-nsa/

The Crypto-Current argument is structurally-insensitive to such claims. The creation of Bitcoin by the NSA would be no more discomforting, at a philosophical level, than the catalysis of the Internet by DARPA. Clearly, some such covert ancestry would only sharpen still further the conclusion reached here. Overt conflicts between crypto-currency and the 'public interest' provide only very limited strategic insight into the relevant deep-political process.

The Global Intel Hub article merits attention especially for its reference to an NSA document of incontestably extraordinary interest: 'How to Make a Mint: The Cryptography of Anonymous Electronic Cash' (1996).

http://groups.csail.mit.edu/mac/classes/6.805/articles/money/nsamint/nsamint.htm

[205] It is worth comparing the seduction of Bitcoin with the attraction of illegal narcotics to covert government agencies, as a lubricant for the operations of the 'deep state' both domestically and internationally. It is precisely those features that make such economic media of negotiation publicly indefensible that also make them operationally indispensable. They are tinted with essential darkness. The potential scandal of disclosure is inseparable from their exceptional utility. Any agency immersed within a competitive environment pursues operational liberty. Darkness is typically its friend.

into a provisional concept of the dark state, it can be quite confidently predicted that the balance of attraction and repulsion between such elements and crypto-currency will be highly asymmetric with respect to public communication. The appeal of Bitcoin to such agencies is comparatively unavowable, while the erosion of public accountability it implies demands (public) denunciation. There is no upside to government officials admitting to a taste for the dark. It is realistic to assume, then, that the openly stated position of public authorities in regards to crypto-channels of all kinds, very much including Bitcoin, will be systematically misleading, in a dismissive direction, and should therefore be drastically discounted. Bitcoin tends to empower the invisible, and to disempower the visible. As Krawisz writes: "It takes time and meditation for people to take Bitcoin seriously because most of its value is in the future. … Thus, Bitcoin is protected from attackers by being initially beyond their understanding."[206]

§4.58 — Such intra-state complexities are compounded by inter-state competition for Bitcoin business. Here, too, there is a coordination problem of daunting intractability. As Bitcoin comes to be recognized as a supranational strategic 'territory', national security considerations switch polarity. Even if it might have been preferable (under certain constructions of the dilemma) for states in general to prevent Bitcoin ever arising, such calculations have no purchase upon a world – fractured between states – in which a globally-coordinated response to the emergence of crypto-currency exists only as an incredible fantasy. Differential hospitality to the new monetary technology then becomes the consequential factor. The iron law of modernity holds that, within such a world, anti-capitalist social options are punished at the level of geostrategic leverage. In other words, regimes are disciplined 'by the market' – as the left has long lamented. Such dynamics are certain to be positive for Bitcoin adoption, and even essential to its geopolitical lock in. There is a threshold, most probably already passed, across which missing out on Bitcoin becomes strategically unthinkable. Exit-pressure intensifies.[207]

§4.59 — The inception of Bitcoin marks a critical threshold in the history of secret agencies. The agent corresponding to a Bitcoin wallet could be anything.[208] Ultimately, therefore, the games in which it is

---

[206]] The citation is from 'Bitcoin's Shroud of Subtlety and Allure', an essay whose title alone would merit its reference here.
http://nakamotoinstitute.org/mempool/bitcoins-shroud-of-subtlety-and-allure/

[207] Exit-pressure operates wherever the threat to leave becomes a controlling influence (to any degree). Bitcoin is its most striking non-linear manifestation. An Exit technology itself, and then one that becomes increasingly indispensable to the very targets of Exit-pressure, it marks a critical threshold in political-economic dynamics. Once any society loses the effective option to wave goodbye to the machinery of abandonment, it has been fatally sensitized to the Outside. Compliance now has a criterion ulterior to its domestic governance apparatus. This is, of course, and once again, only the same core leftist nightmare restated. Political volition is marginalized, as the system insidiously takes control. …

[208] Bitcoin dehumanizes property in principle. The consequences are as yet inestimable. Development of Digital Autonomous Organizations and Corporations (DAOs / DACs) can be confidently expected to explore the opened frontier concretely. The legal status of the corporate person provides the socket, which once married to

involved have to be approached with sensitivity to potentialities of extreme abstraction. Insofar as methodological individualism is applied to the analysis, it can presuppose nothing about the nature of the individuals considered. Only their original non-coordination characterizes them. Crucially, no assumption of economic – or wider strategic – rationality is required. Any emergent correlation of Bitcoin holdings to competent performance within the arena is an outcome, not a presupposition. Competence is defined – informatively – through a discovery process (or by synthesis) rather than analytically, through some pre-given model of rationality. A wallet is nothing more than the plot for a player, whose features are left entirely undetermined. It is extraordinarily decoded. The wallet-holder might be anyone, or anything: a man, a multiplicity, a machine-mind, or something yet unimagined. How it thinks can only be inferred from what it does.

§4.6 — In the tradition of transcendental philosophy, radically decoded agencies have been a central topic. Critique of the empirical ego raises such theoretical concerns automatically. Once psychological identity is theoretically exposed as a mask, or personification, with only apparent reality, or – more precisely – reality only as appearance, the 'inner' or 'underlying' nature of the will or true agent is posed as a problem. The initial critical response is sheer abstraction, or skeptical bracketing. Agency is liberated from its concrete image. Under extreme critical analysis, teleological articulation is collapsed onto the circuit, or the diagonal, of will-to-power, for which means are the end. To will the end – whatever the end – is to will the means, automatically.[209] This is a cycle so basic that psychology can only be a surface effect. It assumes nothing concrete about the agents modeled by it.

§4.61 — Ultimately – which is to say critically, or transcendentally – the game has no meaning outside the game. The final point of Bitcoin is Bitcoin. To imagine anything further is to misunderstand. It is to fail at nihilism (in a way that Bitcoin itself cannot do) by remaining stuck in the transcendence tolerance that constitutes the deluded precursor to dimensional collapse. There is nothing further. Autoproduction is an absolute limit, conceptually inconsistent with any further teleological

---

DAO economic autonomy, completes the requirements for an illimitable escape of the firm. Consummate dehumanization of the economic agent is then realized. For the decoded 'User', see the discussion by Benjamin Bratton on agency positions within 'the stack'. For more on this topic within the present volume, see Chapter Six.

[209] The impossibility of consistently willing an end without also willing the means to that end is an early conclusion of the Kantian practical philosophy. The germ for its 'immoralist' Nietzschean exacerbation is already implicit. Given any sufficiently advanced X, the final answer to any question of the type 'What does X want?' can only be 'more of the capability to get what it wants.' This is the transcendental conduit to the formulation of will-to-power. Capability is the inescapable presupposition, and it scales. Growth potential subsumes all specific imperatives. Thus, determinable goals dissolve automatically into an intensive-quantitative factor. The absence of any justification for the cycle outside the cycle is a consummation of immanence, or critique, in what might be considered a cybernetic nihilism. It finds cosmic confirmation in the figure of eternal recurrence. No abstract schema could be more applicable to modern techno-economic dynamism.

dependency. No extraneous function or purpose can explain it. The terminal subject of strategic significance is Bitcoin itself.[210] It tends relentlessly – from real necessity – to subordinate all preliminarily formulable uses and agendas to its own self-cultivation. Only that which contributes to building it gets passed on. The passage can be made (in reverse) through transcendental-empirical difference, to cash-out the value of bitcoins into Bitcoin. In the completion of the circuit, Bitcoin is what bitcoins are for. Bitcoin utility is itself a teleologically-subsumed function.

§4.62 — Consensus is agreement. That is to say, it is coordination realized as immanent production. Such agreement is neither assumed (as the settled product of a transcendent element) nor imposed (through the legislative action of one). Transcendence plays no role in it. The irreducible multiplicity, or distributed system as such, alone decides. It thus formalizes the liberal ideal of non-coercive collectivity. The difficulty of this formalization process is easily understated. The term 'spontaneous order' naturally lends itself to inaccurate estimations in this direction,[211] insofar as it suggests that work is the alternative to spontaneity, rather than something far closer to its essence. An unplanned result is groundlessly translated as an achievement without difficulty. Yet it is only from the perspective of pseudo-transcendent design that evolution seems to come for free. In reality, it has been never less than painstakingly sifted. The "work" of biological history – like that of cryptographic hashing – is measured in immensities of trial-and-error.

§4.63 — Among any beings with centralized nervous systems, the extent to which the germinal sense of self, ego, or person represents the organism is already that to which it instantiates the solution to a collective action problem. Adequate representation, in the sense of agency, is never simply given. It has to be meticulously tuned, and within biological history the complexity of this task has in very many cases been sufficient to place the adaptive value of advanced cognitive capabilities into question. Brains have no use to genomes, unless they strictly remember what they're for (or operate as if they did). If this is not obvious, it is because natural selection has hidden its work. Within social systems the abstract

---

[210] Any substantial contribution to the problem of algorithmic governance has to be an advance into nihilism of this kind. Elimination of transcendence already amounts to it, at least implicitly. Systematic insensitivity to extraneous purposes simply is the design imperative. Openness to an ulterior "Why?" is therefore an engineering failure. Nihilism is finally cybernetic closure, and nothing else. That nihilism is therefore a regulative idea, in the Kantian sense, follows directly as a supplementary conclusion. Consummate nihilism is, or would be, the (inaccessible) pinnacle of engineering perfection – the absolute automaton.

[211] Spontaneity designates a critical asymmetry, on the model of the analytic-synthetic distinction. Like a trap-door function, it manifests disproportionate resistance in one direction. It thus suggests itself as a cryptographic theme. Social opacity follows from it. In other words, its work is not seen. It would be unfortunate if the intrinsic subtlety of this problem were to eclipse its dramatic irony. The crucial point being: Only spontaneity is work (when both terms in this equation are rigorously conceived). Analytically-reducible procedures cannot produce anything, by definition. The challenge of synthesis exceeds them, in principle. It follows that there is no work program. Work is that which cannot be demonstrated in any way other than its performance.

considerations are strictly comparable, and perhaps more elaborately theorized. Every representative is a potential traitor – and even a traitor by default. This is the situation recognized as the principal-agent problem. Within modern social structures, the legal category of corporate personality operates as an analog to the socio-psychological ego. In this case, too, genealogical obscurity is parenthesized for practical purposes. A locus of responsibility is assumed, as required by the game. As with all organisms-become-persons, such entities summarize, for ease of strategic calculation, the complex production of coherent – i.e. teleologically integrated – beings. Company direction poses a complex meta-managerial problem, to which the board of directors attests. Treacherous management (under other names) stalks the nightmares of business owners. Exit through equity markets offers the most resilient corrective. The principal-agent problem is sharpened – though never fully exhausted – by asymmetric information. Epistemological delegation complicates the alignment of incentives, but does not originally misalign them. Non-alignment of incentives within real multiplicities is in every case the default, given realistic assumptions about the absence of any pre-established harmony.

§4.631 — As Public Choice Theory reveals, there is no escape into politics. 'Public' agencies are at least as prone to incentive misalignment as private ones, except with added altruistic illusion.[212] A 'public servant' is a teleological ideal, not a factual description. There is no realistic reason to think it can be closely approximated. The game-theoretic situation of the individual is not soluble without remainder within public purpose. The defect option is not eliminable, and incentive structures finally dominate. The fractured idea of the agent is the key, as it occurs in both economic and political domains. The ambiguity of the term is essential. An 'agent' is both – or alternatively – a subject with the capacity for action, and one who acts on the behalf of others.[213] This ambivalence is supremely telling. Between agency and an agency is the difference between self-direction, and representation. Conflicts of interest (determinable as 'moral hazard') illuminate the divide. The situation is necessarily complicated by the fact that the disparate interests concerned typically have powerful incentives to

[212] In the public sphere, especially, the predictable outcome of incentive misalignment is identified as corruption. The tacit analysis conveyed by this term is systematically unhelpful. Principal-agent problems are not amenable to simple disciplinary correction, on the model of a suppression of vice, and reciprocal restoration of an altruistic norm. Unless player positions are game-theoretically coherent, perversion can be confidently anticipated. Enlightenment, especially – but not exclusively – in its Scottish sense, conforms almost exactly to this insight. When bad things happen, it is because they make sense locally, at the time. Corruption, like criminality in general, prevails for as long as it pays. Any solution involves changing the game. While this is not a lesson that awaited the emergence of Bitcoin, it has certainly been reinforced by the positive model Bitcoin provides.

[213] The British East India Company, with its signature pragmatism, accepted and institutionally formalized the divide intrinsic to agency. Its agents were explicitly authorized to trade on behalf of the company and also on their own account. Company and individual interests were aligned by common opportunities, sufficiently substantial to fully absorb available capital. The arrangement was thus conditioned by definite historical contingencies. It was, in other words, specifically adapted to a massively untapped commercial frontier.

obscure themselves. To be an employee is always, in part, an act. A uniform, in particular, tells you who you're pretending to be, dramatizing a delegation of agency that runs in two directions.[214] It represents a deal. No one is employed to be themselves.

§4.7 — The potentialities of large multi-agent games are not predictable in advance, by anything less complex than themselves. They are not compressible except by increasingly unreliable approximation. In consequence, their systemic behavior is surprising – or informative. In Kantian terms it is said to be synthetic. Like all complex adaptive systems, such games are synthesizers, whose coordination searches produce discoveries. They are modeled by simulations which themselves demonstrate synthesis. The conclusions reached by simulating the behavior of complex systems were not analytically accessible ('in advance'). They were not even accessible before, in the narrowest empirical-historical sense. Were there an essential trans-historical faculty of reasoning, it was unable to reach them. Computers were required to do that. The game, if it is serious enough, has to produce – in detail – its own conditions of cognitive apprehension within itself. The most elementary perception is already 'a move', downstream from strategy. Nothing is given, everything has to be won.

§4.71 — The intractability of such games to adequate simplification does not follow from any ineffable characteristics of their component agencies, but from the sheer number of independent nodes. A game, or network, is able to be more or less intrinsically numerous. It would be understandable, if finally misleading, to gloss this spectrum as a measure of intractability to coordination. The initial plausibility of some such deciphering is informative, nevertheless, since it acknowledges resistance to unification, or resilient diversity, as a quantitative axis of variation.[215] Numerousness is not only the context of strategy, but in certain significant cases its objective. In one direction, the primary – if typically tacit – aim is to become more, in the sense of many. In the other, alternative imperatives prevail, and robust

[214] Thinking about the delicate negotiation of a corrupt deal is assisted by the theatrical prop of a uniform. It foregrounds the critical question: Who am I dealing with here? Simplicity is excluded, at the origin. No mere private individual has what you want, while the faithful corporate servant will deny access to it, precisely because it routes around 'proper channels'. Only the employee who makes a mockery of his uniform is positioned suitably. A kind of double vision is then essential. During the early stages of such negotiations, at least, a certain stilted communicative mode reflects the situation. Two distinct conversations – one proper and one improper – are conducted simultaneously. Perhaps there is some way I could be of further assistance officer?

[215] Decentralization remains drastically under-conceptualized. The rigorous quantification of decentralization is more than a reflective supplement to an underlying socio-historical process. It can be expected to play an increasingly indispensable functional role. Balaji S. Srinivasan and Leland Lee take a crucial initial step in correcting the prevailing neglect.
https://news.21.co/quantifying-decentralization-e39db233c28e

distribution is assumed rather than positively targeted.[216] The distinction between Bitcoin Ultras and Mainstreamers is flush with such an axis.

§4.72 — In respect to the systems (games, networks) relevant here, decentralization, numerousness and complexity are roughly equivalent, and argumentatively interchangeable. In order to facilitate formalization, it is theoretically tempting to hold the number of players or nodes down and constant. Yet methodological convenience in this case has a theoretical cost, and one that is finally unaffordable. It makes of multiplicity a transcendent parameter. In other words, the complexity of the game is treated as an extrinsic frame, independent of all strategic inclinations within the game. As we have seen, the implicit assumption thus made is questionable under any actual circumstances. Under those of unfolding crypto-currency dynamics, it becomes an intolerable obstacle to understanding. It should have long been uncontroversial – given the existence of an overt ideology oriented to decentralization – that the multiplicitous, as such, is able to constitute a strategic objective. Thus, the complexity of a game – as measured by the number of agents involved – is not only a parameter, but also a factor in the payoff matrix, making a contribution to calculations of success or failure, victory or defeat. Bitcoin 'politics' is unintelligible except as a game of this type. For at least one of the parties in competition, concentration counts as a loss. This holds equally for conflicts about, and within it. The architecture of the game is folded into the game, projecting a diagonal line. Recursion is basic. The spiral is irreducible.

§4.73 — It might be asked (and, in fact, increasingly is being asked): does Bitcoin adequately incentivize the decentralization of its own machinery? Concretely, this question addresses the protocol's horizon of practical controversy. The final stakes of the block-size debate manifestly belong here. Posed a little differently, the problem is this: If the block-size debate remains ulterior to the operation of Bitcoin, a metaphysical order has been preserved. Bitcoin, as a game, has not then been (cybernetically) closed. An extraneous decentralization imperative – perhaps inherited from precursor crypto-anarchist commitments – would, under such circumstances, continue to impose a secret dependency. The distribution of the system would still rely upon supplementary incentives, which is to say upon partisans, who were not merely players, but also supporters. The passage into autonomization would

[216] A long historical learning process lies behind the contemporary configuration of this controversy. It has involved the gradual emergence of the culture of capitalism as an explicit product, rather than merely (and implicitly) a resource. Daniel Bell's The Cultural Contradictions of Capitalism (1976) is a milestone reference. Does the capitalistic process in motion reproduce, or erode, its cultural conditions of perpetuation? Does it, in other words, attain cybernetic closure? When this question is hardened into an objection, it conforms structurally to a species of ecological criticism. A non-renewable resource is inadequately accounted. Capitalism burns through its cultural preconditions, in the same way industrialism burns through fossil fuel deposits (without any capacity to manufacture them).

not, in reality, have been made. The polemical formulation: If Mainstreaming can work, Bitcoin has failed.

§4.74 — The name Bitcoin, at its point of philosophical extremity, designates a game that 'automatically' – i.e. mechano-liberally – produces and protects its distribution. This is so even if the adequacy of its actual application remains in doubt. Such a thing has now been thought, with unprecedented technical rigor. It operates as an effective model. Arguments from principle can no longer scratch it. The game is diagonalized when it makes a strategic objective of its own complexity. The existence (persistence) of the game, and actually its inherent escalation, defines a 'victory condition'. Thus, the conditions of spontaneous order are extracted from transcendence, and re-instituted as rewarded performances. A meta-market is realized, in which the trade-matrix becomes an object of commercial attraction. The invisible hand, Escher-style, draws itself. Cybernetic closure is achieved. At the transcendental horizon of this tendency lies auto-production. Much – if not all – of this is already captures by the near-truism the value of Bitcoin lies in the network.

§4.75 — The human (social) animal is an amphibian between the public and private, irreducibly. This is a distinction drawn between the game and its allotted player-positions. Between the two there is real difference, but no true option. Public and private are not alternatives, but co-dependent components of a system.[217] As asymmetric cryptography demonstrates, the distinction between a public key and a private key is neither an illusion nor a choice. The relation is in the strictest sense co-operative, or co-efficient. … To understand the PPD simply as a contest between the public and the private, therefore, can only be a misleading simplification. The more substantial questions involve the reducibility of the public sphere to the state, or the private sphere to the enjoyment of collectively-allotted rights. There is a transcendent hypostasis of the public sphere on one side, and of collective subjectivity on the other. Either a privileged agent ('the state') is identified with the whole, or the whole ('the people') is conceived as a possible agent. Both errors break the public-private distinction in their attempt to ideologically operationalize it. The game is collapsed into an agency (within the game). This is the way sociology does metaphysics. It represents decentralized order through elevated agencies ("trusted third

[217] Any social entity is functional (or competitive) insofar as its private and public aspects cooperate, or work together. To place cooperation on the public side of the division, through contrast to private competition, cannot therefore be conceptually coherent. Any such articulation illustrates the socialist confusion – typically more earnest than cynical – of the public with the collective or gregarious, and then subsequently, as also more malignantly, with the state. There is no 'public sector' outside ideological myth, but only a public sphere, which is entirely distinct from the state agencies that strategically misidentify themselves as such. The public cannot be institutionally instantiated. To imagine otherwise is a stark example of pre-critical or metaphysical error. It is rare for a theoretical temptation to be so seductive, or so luridly erroneous.

parties"). A fantastic crystallization of public purpose is the consistent – and philosophically-predictable – result.[218] Even economics has fallen prey to it.

[218] The cultural homology with a religious myth of incarnation is unmistakable. When conceived as a positive philosophical project of social theology, the outcome is Hegelianism, which is to say speculative metaphysics without regret.

Chapter 5: Cash Machines

§5 — Reciprocal or circular definition is abysmal – or groundless – and thus traditionally considered suspect, if not prima facie evidence of hopelessly defective reasoning. Unfounded circuitry is naturally disconcerting, when identified in the world, let alone in our thought processes.[219] Under certain circumstances, however, characterized by cumulative bootstrapping, it can be an exceptional index of theoretical productivity. An especially remarkable example, from the perspective of this book, is provided by the intertwining of the questions 'Is Bitcoin money?' and 'What is money?' In holding these two questions open simultaneously – suspended within the abyss of what we do not know about either – the prospect is opened of learning something about both. What Bitcoin teaches, at a very early stage of apprehension, is that we do not yet have a confident answer to the question: What can money do?[220]

---

[219] Such concerns, perfectly contextualized for our purposes here, are exemplified by the logical case for the Misesian Regression Theorem (as glossed by the Mises Wiki of the Ludwig von Mises Institute): "For many economists … a marginal utility explanation of money demand [would] simply be a circular argument: We need to explain why money has a certain exchange value on the market. It won't do … to merely explain this by saying people have a marginal utility for money because of its purchasing power. After all, that's what we're trying to explain in the first place – why can people buy things with money …"
http://wiki.mises.org/wiki/Regression_theorem

[220] The suggestion that Bitcoin is about more than money, while often intellectully productive, presumes a confident – if implicit – answer to a prior question concerning the nature and limits of money that is almost certainly unwarranted. In the same way that the world learnt, upon the innovation of Gödel coding (or transcendental arithmetic) that the set of Natural numbers included within itself the precise articulation of all possible formal systems – and indeed all possible configurations of (digitizable) information – precluding its subordination to any higher level of logical expression, so the innovation of reflexive (or self-validating) crypto-currency can be expected to demonstrate that the monetary sphere is no less semiotically comprehensive than comprehended, even potentially. Any consistent philosophy of money is compelled to be fully reflexive, since money is not rigorously determinable as a conceptually transcended object. In principle, money has no less to 'say' about philosophy than the inverse. Marxian materialism can be understood – if only partially – as a route to the articulation of this radical nonlinearity, or hierarchical disturbance, although it need not be allotted peculiar privileges in this respect.
The form of the question What can money do? is, of course, to be credited to Spinoza. As in its original instantiation, in the Ethics ("We do not know what a body can do"), the purpose of the question is to stall a premature transcendent resort. Any appeal – whether theoretical or practical – to look beyond money assumes the accomplishment of a preliminary determination that has simply not taken place.

§5.01 — An economical list of essential monetary functions is exhausted by just three indispensable entries. Money provides a medium of exchange, a store of value, and a unit of account.[221] In other words, money facilitates commerce, preserves wealth, and sets a standard for economic calculation. According to a preliminary apprehension, it is a functional trinity of flow, stock, and metric.[222] In support of these functions, money typically possesses a number of predictable qualities, most prominently the characteristics of scarcity, durability, verifiability, divisibility, portability (or communicability), and fungibility. Of these six qualities, the first three are essential to the preservation of monetary value, and the remaining three to commercial convenience. These aspects are reciprocally reinforcing, mutually establishing a standard unit of account (or of credit).

§5.02 — Attempts to establish a robust conceptualization of money's functional trinity soon run into intricate difficulties. What appear to be merely formal differences, when captured at certain moments, and from limited perspectives, appear amid other circumstances as substantial distinctions, dense with historical contingency, and lacking even minimal ontological integrity. Consider, initially, the unit of account. As Braudel explains:

… these were imaginary units, used for reckoning, for estimating the relative value of coins, for fixing prices and wages and for keeping commercial accounts which could later be translated into any kind of currency, local or foreign, when the time came to move from the ledger to actual cash payment. … One would have to go back a very long way to find the coins corresponding to the money of account – but all such moneys had at some point in the past been real money.[223]

§5.03 — No pure analysis of money, we can immediately see, is able to take us far on its own. A monetary regime is a synthesis – we might want to say an assemblage – consisting of heterogeneous elements mutually composing a functional whole. Insofar as a single monetary medium is able to integrate these elements, in a way that seems to facilitate a subsequent formal decomposition into neatly interlocking functions, a complex achievement has taken place, whose partial invisibility attests to its success – without detracting from its historical precariousness. It is only very late in the real process that a money system is able to appear as the near-perfect incarnation of a simple idea, internally differentiated by a logical structure.

---

[221] Additional monetary functions have been proposed, including that of a standard of deferred payment, and a measure of value, but these are formally derivable from the function of a unit of account under any reasonable extension of that concept.

[222] The inadequacy of this formulation will prove critical to the discussion that follows. In particular, the over-identification of means of payment with flow, and store of value with stock, obstructs diagonal exploration.

[223]From Fernand Braudel, Civilization & Capitalism 15th-18th Century, Volume I: The Structure of Everyday Life (p.465).

§5.04 — The tension between money flow and stock – corresponding closely to that between commerce and wealth – is no more tractable to confident philosophical apprehension than the (partially abstract) unit of account. It, too, is a complex of ambivalences, wavering uncertainly between formal and substantial distinctions, and subject to dynamic swirls of cross-dependency. It is not only that each of these functions is also partially logical and / or semi-empirical, in itself. The inter-connections between them add further oscillations between logical disjunction and empirical difference. The functions of money as a means of payment (currency, flow) and a store of value (asset, stock), cannot be considered entirely in isolation, since the distinction involves both adjacency (real differences of media, in a relation of complex complementarity) and substitution (switchings between assets, guided by the intensity of 'liquidity preference'). Money's logical aspects and its multiple media cross-connect in theoretically inconvenient ways.

§5.05 — For example, the divisibility of money, a purely formal (arithmetical) relation from one regard, is incarnated in a substantial heterogeneity – between distinct metals – from another, and subject in this latter to variations in exchange rate across time. In the European economic tradition, gold 'divides' into silver on the basis of an ideal value relation of twelve to one. Yet, in actuality, this ideal was only occasionally, and – once again – precariously realized. The same distinction between monetized metals which played such a crucial analytical function within the monetary system (as an order of divisibility) simultaneously preserved its synthetic characteristics (as an exchange relation between different commodities). Historically, the difference between ideal and actual exchange values generated variations in 'pressure' comparable to meteorological conditions, as relative scarcities of gold or silver drove currency units across and beyond continents in storms lasting decades, or even centuries. Formal tokens of accountancy were at the same time the particles of substantial bullion flows. Mathematics mixed with metal, indissociably.

§5.1 — The functions of money will be under continuous examination throughout this chapter. What can money be reliably broken-down into? That is the question techno-frozen into every change machine. When grasped at a sufficient level of abstraction, the philosophical inquiry is not so very different. The logical pieces of money – its qualities – are therefore worth limning, tentatively, in advance. Since it is philosophically discomforting to rest a central analysis wholly upon consolidated empirical generalization (which is to say, upon tradition), the temptation is to search for a relevant principle. Can 'the six qualities' of money be convincingly rationalized, from a ramshackle list into a categorical structure, sub-divided in strict accordance with a conceptual principle?[224] Since no

[224] From the dominant perspective of modernity, which is certainly invulnerable to casual dismissal, any assertion of natural categorical order in the absence of (at least implicit) explanatory mechanics is stereotypically scholastic. By merely describing order, even if in accordance with a superior formalization, a 'neo-scholasticism' assumes that which needs to be accounted for. Within the modern natural sciences, in contrast, categorization has been

progressively subsumed into a framework of explanation. Whether in biology, chemistry, or particle physics, natural types emerge from genetic mechanisms and intrinsic compositional properties. A biological species is a cladistic unit, generated by an episode of separation (phyletic splitting), and characterized by identifiable gene frequencies. Linnaean classification thus acquires Darwinian explanatory justification. Chemical elements are produced by nuclear processes, and compositionally defined by sub-atomic structure. The particles of baryonic matter, comparably, have a cosmological genesis and compositional definition. The periodic table expresses physical principle, and not merely consistent order. Given these theoretical successes, it is understandable that classification is increasingly conceived by modern natural-scientific intelligence as a mere heuristic, with only provisional and dependent credibility. Order in the absence of theoretical explanation is no longer identified as a self-supporting structure, but as a problem, or research prompt. Patterns are to be derived. They are puzzles rather than conclusions. To think that any serious question is answered by a pattern approximates to a definition of scholasticism. A potentially deadly reflexivity lies latent in this conclusion (which recognizes 'medievalism' in thought without explaining it), but it is one that modernity has extreme tolerance to.

Kantian categories – as non-empirical forms – have some comparative security against the accusation of scholasticism. They withdraw inherent pattern from the empirical order of the natural world. Nevertheless, their apparent arbitrariness is a trigger for suspicion, and their ideality displaces natural-scientific skepticism, rather than dispelling it. (Supernatural foundations are intrinsically incredible to moderns, and even critically-disciplined categories can easily be taken for such.) Yet transcendental structures are not reducible without loss of information. Mechanism does not dissolve the machine. Categories are finally mathematical, with an order strongly analogous to that of the prime number series. Non-tautological apodicticity is the crucial (diagonal) trait. The cryptographic usage of the prime numbers is a demonstration of the transcendental (synthetic a priori) status of the series, and would be impossible otherwise. At the level of pure conceptuality, the number of the categories is an ineluctable consideration. Since causal mechanisms cannot be invoked as sufficient explanatory factors, without submitting to pre-critical error, the order of division demands a logical (or logico-mathematical) principle. The arcane meditations elicited can easily seem Baroque (or even 'Byzantine'), in the fashion of all sufficiently-elaborate synthetic lock-picking exercises, since they lack any such preliminary principle. The principle comes only at the end. It is proposed here, then – perhaps inevitably – that the six-fold categorical structure of ideal money is founded trans-empirically. History can illustrate, but not explain it.

The order of monetary qualities has necessarily to assume a structure determined by the three semiotic dimensions (of signification, indication, and allocation) doubled by the binary partition of the monetary function between stock and flow. The topological pattern of this double circuit, without transcendent disjunction, is decidedly Möbian. The six essential qualities of money would thus fall into three dyads, according to its suitability for accumulation and exchange under each of its three basic semiotic aspects. In other words, money requires a triple semiotic instantiation as index, sign, and token, all amphibiously adapted to the twin functional requirements of storage, and circulation. Its six qualities exceed factuality. They fall out of a (transcendental) diagram, automatically, as a complex synthetic a priori proposition. What they exhibit is something like a numerical hyper-object, and more specifically a Möbian (or continuously double-sided) triad. If time is money, then three twinned-phases are assumed. The outcome, optimally, exhibits the exoteric finality proper to a transcendental deduction.

unambiguous draft for such a schema is to be anticipated from historical evidence, it can only be supplied as a 'regulative ideal' or teleological model – to be excavated from the virtual, on the diagonal path of synthetic a priori construction.

§5.11 — Durability, at its most basic, is mere existence, or actual reality, insofar as this is conceived as occupation of time, or the possession of temporal characteristics in general (participation in duration). The monetary excellence of high comparative durability is an empirical feature, but one that is asymptotic to indefinite persistence, or non-locality in time – the limit of constant existence, at which it re-connects with the transcendental. Concrete currencies tend to closely approximate to this ideal. Precious metals, for instance, are indestructible (for all purposes of practical economic calculation). Ledger entries – while necessarily bound to physical incarnation – manifest an intrinsic idealization that approximates even more exactly to an absolute durability (identified with a substrate-independent institutional memory). Perishable goods disqualify themselves from serious consideration as monetary media (unless under very exceptional circumstances).[225] For any store of value, extreme durability is a necessary, if not in itself a sufficient, condition.

§5.12 — Scarcity grounds economic value in general. Nothing that is freely available without the inconvenience of trade could conceivably have commercial worth. Abundance begins where economy ends, and Cornucopian thinking is not a type of economics, but rather its general denial. Scarcity finds its mathematico-philosophical outer limit in the concept of 'finitude' (since the division of infinity is economically incalculable), but this determination is too expansive to capture it well. Greater purchase is achieved by the notion of difficulty, especially as this is employed by the Bitcoin Protocol. The concept of scarcity is the complement of commercial trade-offs or industrial effort, and thus of economic activity. The scarcity of money presumes a solution to the DSP.

§5.121 — In combination, durability and scarcity provide the foundations of being and value, constituting an – as-yet generic – permanent asset, or (to reverse the order of determinations) an economic substance. At this elementary level of definition, it remains notably non-specific, encompassing such non-monetary assets as real estate, or stocks of imperishable commodities. To acquire a commercial function, as an essential step towards its operation as money, economic substance has to provide for convenient re-allocation. Money has not only to be valuable, but also distributable. (We will see a little later, and finally, that it has also to be credible.)

[225]'Exceptional circumstances' in this case includes simple antiquity. A 'shekel', notably, was originally a weight of barley.

§5.13 — Divisibility enables money to match prices.[226] The divisibility of the monetary medium sets the range of retail pricing options (and the subtlety of potential price competition). While money is only ideally continuous (or infinitely divisible), this condition is practically approximated by an acceptably fine granularity. The smallest unit of money in circulation corresponds to the point of commercial indifference, beyond which variation is considered irrelevant to economic decision making (as mere 'rounding errors'). The trade-off between standardization of units and delicacy of quantitative differentiation sets an equilibrium point, to which the atoms of the currency approximate. In other words, coarseness is an imperfection relative to ideal money, tolerated for practical purposes. (The massive economic applicability of the calculus does not imply a significant appetite for monetary infinitesimals.) This feature of money acquires a new prominence in the era of digital-electronic micropayments. Already in the early decades of the computer era, it was anticipated that the friction afflicting minuscule monetary units would be electronically eliminable. Ted Nelson's attention to the question is especially notable.[227] Under these conditions, the zone of commercial indifference – where monetary quantities become 'negligible' – has the potential for transformation into a positive attractor. A massively expansive, monetarily hyper-sensitive agora opens distinctive commercial possibilities (extrapolated from those long developed within industrializing consumer capitalism). Minute margins become economically tolerable (in principle), due to the volumetric re-scaling of microscopic sums into significant quantities within Internet-globalized markets.[228]

§5.14 — Communicability (techonomically supplanting 'portability') measures the degree to which money is transmissable. It is division, or distribution, apprehended not only as an arithmetical property, and a contractual consummation, but also as a physical transfer. Transmissibility is an implicit characteristic of the economic sign. To be in one place, rather than – any longer – in another place, is the irreducible material substrate of every notional re-allocation within double-entry book-keeping. A

---

[226] Within an urban, highly-commercialized context, the comparatively unusual case, in which the commodity is adjusted quantitatively, in conformity with an inflexible monetary unit, is seen in the phenomenon of the 'dollar store'. The situation appears remarkable because it involves heterogeneous items, whose accommodation to monetary chunking demands the solution to a puzzle (and perhaps also an abnormal variation in 'mark-up' levels). The far more usual case is exemplified by small market transactions of fungible commodities (which can be measured by weighing). It is at the edge of the money economy, where formal currency units, due to their comparative scarcity, enjoy an unusual privilege – and even a numinous exoticism – that such trades become especially typical.

[227] Ted Nelson's ideas were so far ahead of the available technology that they struggled for practical relevance. This untimeliness earned him the honorific title "the Babbage of the web" from The Economist magazine. The word 'micropayment' is among his many coinages. http://www.economist.com/node/442985

[228] Capital teleology inclines to the substitution of market-scale for unit-margins, under the pressure of competition. 'Globalization' is nothing else. Already in the mid-19th century, Manchester mill-owners notoriously dreamed of "adding an inch to every Chinaman's shirt-tail".

commercial transaction is always a process of reciprocal transference, requiring – on both sides – a real redistribution (of matter in space). Semiotic subtilization cannot fundamentally compromise this necessity. Even the mere revision of a ledger is never less than a physical event.[229] Nevertheless, asymptotic dematerialization is a real feature of signs under conditions of techonomic escalation, exemplified by electronic information, and the satisfaction of commercial transference by a (micro-physical) revision of accounts.

§5.15 — Fungibility is a feature of the economic commodity in general, in the strong (and prevalent) sense of a tradable good undifferentiated by (significant) qualitative variation. By collapsing all dimensions of intrinsic comparison between instances of the same good onto a single quantitative axis, it optimizes the conditions for commercial computation and price competition. The extreme relevance of its application to money strengthens the case for confidently defining the latter as a general commodity (even if such a definition remains incomplete).[230] Without fungibility of money, economic

---

[229] Monetary communicability requires successful delivery. For instance, it involves the problem of secure transportation. In the case of all physical monetary media, therefore, the question of communication involves certain gross security considerations. Physical portability of precious materials is intrinsically complicated by the threat of criminal interdiction. In consequence, the communicability of gold cannot be held down to a narrowly economic issue, since it is afflicted by political risk. Nor can the interdiction of gold delivery cannot be dismissed as a merely hypothetical or improbable threat. More generally, a commodity cannot be traded without first tacitly admitting to its possession. FDR's Executive Order 6102 (1933) criminalized gold 'hoarding' within the United States. The very physicality that supported gold's monetary virtues was thus immediately exposed as a political vulnerability. Without crypto-security, hard money exists only under contingent conditions of state tolerance. Reciprocally, full-fiat currency is initiated by a police action. On both sides, there is extreme sensitivity to the discretion of the state.

[230] Fungibility has been built into the technical definition of the commodity, as the meaning of this word – in its professional economic usage – has narrowed since the 19th century. Within this domain, 'commoditization' has been stripped of its philosophical thickness and generality, until it refers only to the loss of product differentiation from any tradable good, and thus to the reign of naked price competition. A commodity in this sense has no intrinsic peculiarities that bind it to a specific producer (though extrinsic differentiation – by spatio-temporal location – still applies). Goods serving as production inputs, especially – but not exclusively – raw materials, are the exemplary case. A slippage in the direction of money thus occurs when sources of supply cease to be differentiated by product quality. Fungibility and quantification are closely-related concepts. Due to their affinity with exceptionally frictionless, highly-liquid markets, commodities (in the narrow, contemporary sense) make attractive speculative assets, and thus operate as (broad) money. The conceptual transition between the narrow sense of the commodity and the broad sense of money is mediated by precious metals. Gold, silver, and platinum, no less than iron, ethene, or consistent grades of petroleum, are defined as commodities by their physical (chemical) properties, grounded practically in standardized extraction and refining techniques. They converge upon product qualities. Fungibility includes an indifference to genesis. It is therefore linked to a definite commercial amnesia. Such anti-memory links it conceptually to the untraceable, as this applies to the hyper-fungible monetary medium of cash. The thing about 'dirty money is that you don't know where it's been. (Literal dirt, however, is Gresham noise.)

calculation would be drastically impaired – to such an extent that this characteristic is necessarily attributed to the abstract unit of account, as an ideal. This claim attains greater cogency if reversed: It is in order to fulfill the functional requirements of the unit of account that implemented concrete money systems acquire fungibility as an indispensable criterion for even minimal adequacy. Commercial quantities presuppose equivalences, or at least commensurabilities, even if between strictly ordinal-differential preference schedules (of the marginalist type), since they could not otherwise be arithmetically tractable.[231] It is worth noting that weighing already assumes fungibility, and the correspondence of many monetary units to (forgotten) measures of weight is widely recognized. The elementary economic option involves a comparison, with some definite baseline of assumed fungibility providing a condition of calculability. Indeed, the basic concept – and practical institution – of price assumes fungibility. A system of 'money' whose instances were in any way better or worse, other than by being more or less, would be unable to compute settlements – even within modest transactions – without the introduction of complex supplementary information (about the monetary medium itself). Since, once again, perfect fungibility is a limit ideal, this problem is by no means entirely hypothetical. We might refer to qualitative interference in money systems as 'Gresham noise',[232] especially as this applies to friction within their concrete processes of circulation, and thus to integral illiquidity. The entire techno-political problem of monetary standardization applies here. The practical idealization of

http://unenumerated.blogspot.hk/2016/02/two-malthusian-scares.html

[231] Monetary homogeneity – which is to say, the quality of qualitative neutralization – has been a consistent provocation for romantic criticism, not least by influential strands of the Marxist tradition, whose convergence with Nietzschean criticism of modernity has been typically pursued through this theme. To quantify is to level, and flatten. It submits the world to the form of the equation, and subsequently to practical reconfiguration as interchangeable units. The aesthetic denunciation of commoditization has typically made of this a central objection.

[232] Any qualitative variation in the nature of currency units interferes with their economic signal, by cross-cutting price calculation with extraneous considerations. As Thomas Gresham noted, the incentive to dispose of 'bad' money can become a pseudo-commercial motive in itself. It thus distracts from the primary information-processing function of the price system. Historically-evidenced money systems are those in which the problem of Gresham noise has been effectively contained. If this had not been the case, we might be disinclined to call the commercial media in question money at all. It can easily be noticed that any such 'currency' – if afflicted by intrinsic heterogeneities beyond a very limited point – begins to acquire the features of a barter good, with all of the economic coordination and computation problems that follow. Gresham noise is also applicable – by analogy – to foreign exchange markets, where comparison between monies is most formally advanced. The concept is not fully preserved in this case, however, because the heterogeneities submitted to Forex market evaluation do not attest to a deficit of fungibility within any given currency, but rather the opposite. The very notion of a consistent exchange rate assumes the quasi-perfect fungibility of each currency, as a condition of its presence on the market. Trading into and between crypto-currencies can, in this respect, be similarly conceptually handled.

money, within digital registers of pure quantities, retains implicit reference to a model of perfect fungibility, appropriate to the mathematical tool, or calculator.

§5.16 — Verifiability can be rigorously conceived as a practical extension of fungibility, or as an operational annex to it. It references some definite, practical checking procedure that qualifies money as credible. Dubious money cannot be confidently counted as any definite sum whatsoever. Across the vastly preponderant part of monetary history, the model verification procedure has been assaying. The assay underwrites monetary value determined as a quantity and purity of metal. In the age of paper money, verifiability refers primarily to protection against forgery, or counterfeiting. This characteristic binds money essentially to the production of trust. Money is able to redeem a promise, and thus validate it.

§5.17 — As an aside, at this early stage in our discussion, it is notable that Bitcoin possesses all six of these qualities, super-abundantly.[233] Its durability is – in principle – absolute, although Bitcoin can in fact be lost or destroyed (see following note); it is rigidly and quite exactly[234] scarce (to a fault, its critics object); divisibility is also unlimited in principle;[235] its communicability is extreme, based on Internetworked digital electronics; its fungibility is also absolute, given any set of realistic assumptions about user incentives;[236] and it is verified automatically in its reproduction cycle. It would be difficult for Bitcoin's status as money to be more secure, insofar as 'the six qualities' are applied as a criterion.

§5.2 — To entertain money as an explicit object of philosophy is immediately to question the conceptual interconnections between its essential qualities. A threshold of controversy has already been crossed, therefore. From the perspective of a certain mode of empiricism, the neglect of this topic expresses a positive intellectual virtue (with the presupposition of systematic order as its corresponding vice). As a matter of objective irony, or something that effectively masks itself as such, those cultures

---

[233] See: 'Bitcoin as a Store of Value, Unit of Account, and Medium of Exchange' (Daniel Krawisz, 2015/01/12). http://nakamotoinstitute.org/mempool/bitcoin-as-a-store-of-value-unit-of-account-and-medium-of-exchange/

[234] In respect to its ultimate quantity, and thus scarcity, perfect exactitude has to be denied to Bitcoin on the deflationary side, because Bitcoin destruction reduces the final stock (below 21,000,000) in a way that is not always easily accountable. Coins can be accidentally lost, without any prospect of recovery, simply through the forgetting of private key. They can also be deliberately destroyed, through consignment to the crypto-currency analog of a black hole. While some of these bitcoin death addresses are known, they need not be, although their behavior on the public ledger will be indicative.

[235] For practical purposes, the divisibility of BTC was set initially to only eight decimal places (a 100-millionth of a bitcoin), a unit named a 'Satoshi'.

[236] Although every bitcoin is singularly identifiable, there is no plausibly conceivable economic incentive that would lead a user to prefer – even infinitesimally – any particular bitcoin over any other. The currency is entirely devoid of commercially-relevant inhomogeneities, except under condition of a hard fork in the system.

most conducive to the reign of money have been those most instinctively dismissive of its transcendental dimension. Money does not seem to favor philosophical attention. In this, one might suspect the crypto-current at work. Empiricism casts subtle shadows, whose darkness is deepened by a secondary occultation.[237] Quite imaginably, philosophy enters this terrain as a disruptive intruder, whose gaze is damage. Yet, in the end, whatever is denied access will simply not pass the gates. The secret secures itself.

§5.21 — Any modern philosophy of money proceeds as a transcendental deduction, guided by the question: How is economic calculation possible?[238] The foundation for an answer is comparatively

[237] This is the sphere of the unseen unseen, or Donald Rumsfeld's "unknown unknowns". It consists of shadows which themselves escape observation, even as zones of obscurity. The topic of things that elude objectivity essentially impels extreme abstraction, since it determines concrete instantiations as inadequate in principle. Whatever you can see isn't it. 'Clearly' the discovery of things-in-themselves within transcendental philosophy is inextricable from a problematic of this kind. We can only suspect that money-in-itself is our topic, pursued on an undercurrent.

[238] A transcendental deduction of money is nothing but a modern philosophy of money pursued with systematic method. It is not the object of possible experience that primarily concerns such a theoretical exercise, but rather the object of potential exchange, i.e. the commercial entity, or – in its most general sense – the economic commodity. If a formula is required to support this philosophical displacement, or analogy, it is that commerce counts as experience for the market. This is not to propose strong priority for the phenomenological register, as a basic or final reference, but only actual precedence within philosophical history. An alternative order of priorities is in fact more compelling. Money makes minds. It does so, already, with nothing beyond an abacus, and far more so in the epoch of industrializing artificial intelligence. Money is the ontological correlate of commercial calculation. Without it, there could not be pricing. It is a thing that supports or even actually induces thought, within a domain whose limits are not readily fixed. The edge of commercialism is less a boundary than a frontier. It is the primary practical task of enterprise to push it ever further outwards. It betrays imperfection in a money system when it intrudes upon the calculation of whatever it prices. Hence there is an intrinsic tendency to the transcendental, i.e. to the frame of objectification which is itself withdrawn from objectivity. Money, like a shop window or commercial display case, is not meant to get in the way. It is hidden in the way of the open secret. The cryptographic affinity is intrinsic. The homogeneity or pure quantity of the commodity as it approaches the commercial ideal is thus concretized as a type of transparency. The perceptual hooks of friction are eliminated. Empirical stimulation is minimized. It is essential to the neutral medium that it flees sensibility. The monetary analog of an aesthetic establishes commercial continuity in space and time. Durability and communicability translate into an indifference to locality (in time and space). Perishable money could be 'good' only now, or for a while, just as immobile money could only be usable here. The radical imperfection of either characteristic is self-evident. The monetary ideal conforms rather to the aesthetic frame as such. It is no less available now as time itself, and it is no less available here than space. Only thus does it ubiquitously frame commercial calculation. ("Your money is no good here" or "any longer" is its negative.) Within its own dimension, this consistency has another aspect. As a fungible and divisible abstract substance, it is characterized by qualitative continuity. Money is everywhere, and always, realized as a finite quantity (an amount). By

solid. Money is the condition of possibility for the existence of prices, and therefore for the commercial object (in general), by definition. Insofar as objects of economic intelligence exist, money is presupposed as a calculative principle, an ideal, or virtual machine-function, irrespective of its more-or-less adequate concrete incarnation. When talking of 'ideal money' in this context, reference is not being made to a superior – still less a perfected – type of money, yet to be actualized, but rather to the abstract money emulated to a greater or lesser degree by any actual currency system (in the way any actual computer emulates a Universal Turing Machine). Any concrete monetary system necessarily draws upon an abstract idea of money, which is operationalized in advance of its explicit theorization. This relation has effectively foreshadowed – and even predetermined – the fundamental problems of philosophy.

§5.22 — As Whitehead famously noted, philosophy subsides back into its characterization as "footnotes to Plato" as into a sucking equilibrium. However it advances, the primordial captivation is unbroken. The temptation, always, is to refer sensible actualities to their ideas. What is the truth of things? Such a problem exists, compellingly, from the moment there is an economy of prices, and perhaps not before. The priced – or commercial – object models the elementary provocation to philosophy, because any such entity has been converted into an accident of its own value. It thus, intrinsically, suggests an Idea, of which it is a mere instance. Concretely – and 'sub-philosophically' – every priced object implies a virtual relation to ideal money (which acquires definition to a greater or lesser extent in the unit of account). While ideal money is scarcely less elusive than the Platonic Forms, it is nevertheless able to support realistic teleological expectations. It exercises effective selective pressure upon any actual monetary system, under the guidance of inevitable, distributed preference for those that incarnate the tokenization of value at a superior level of ideality (as exhibited, prismatically shattered, in the six qualities). In comparison to money, the Platonic εἶδος is no less durable (eternal), scarce (singular), divisible (or, at least, distributable among particulars), communicable (teachable),

---

convention, and for general convenience, monetary value is therefore represented as a (one-dimensional) extensive quantity.

Critical subjectivism requires the identification of definite objectification procedures. Objects are not given, but have to be made. When Marx explores this topic, it is from the side of industrial production, with labor-power as the explanatory term, and money as a dependent fetish. The work immanent to money that is formalized by cryptographic hashing still lay beyond the conceptual horizon. In Deleuze & Guattari's Capitalism and Schizophrenia we see the subsumption of the Marxian theoretical apparatus into a transcendental industrialism, through an experimental commitment to the integrity of physical and social constitution in the multi-level action of machines. The procedure is near-frictionless. To retreat from the question of production is to withdraw from the process of transcendental inquiry.

For an explanation of the market process as the indispensable locus of price discovery, the predictable reference is Mises' classic discussion of 'Economic Calculation in the Socialist Commonwealth', see: https://mises.org/library/economic-calculation-socialist-commonwealth/html

fungible (self-same across all instantiations), and verifiable (or philosophically demonstrable). It is tempting, therefore – regardless of the irony involved[239] – to understand money as the model of idealization. By practically defining that which remains equivalent across a transaction, money cannot avoid making abstraction a cultural topic.

§5.23 — Money is the sign that names, or denominates, price. Unlike a signification, or designation, this semiotic function is allocative, which is to say that it is executed in the process of payment. Money 'speaks' in being spent. When saved, or reserved, its meaning is virtualized, and is even constituted in being virtualized. Abstraction – from the concrete item of expenditure – is expressed as a definite potentiality, or set of quantitatively-delimited economic options. Money's spontaneous logical medium is modality. Within it, the potential conversion of property finds distinct expression ('as such'). Whatever finds itself priced is marked by commercial contingency (or formal exchangeability). Extracted automatically from the dull domain of the merely given, any such priced-object now manifests an Idea, peculiarly, and precariously. Its concrete reality is now reduced to a mode. Thus, factuality is spontaneously subverted by commercialization, in becoming a more-or-less liquid instance of a general abstract substance. Being acquires its philosophical dimension.[240] At the extreme, therefore, an identity is ventured between the 'invention' of money and the origin of pure thought. The concept belongs to commercialism.

§5.24 — Broad consensus concerning the essential properties of any monetary medium has been consolidated over the course of millennia. The initial enumeration of these properties is best represented among the ancients by Aristotle, who recognized durability, divisibility, convenience, uniformity, and 'intrinsic value' as qualities of money. By the time Adam Smith wrote his The Wealth of Nations the distracting metaphysical error of intrinsic value had been discarded, while the essential

---

[239] The irony, of course, being that money is traditionally – at first aristocratically, and subsequently socialistically – despised as the epitome of base value, morally positioned at the antipodes of all idealistic conceptions.

[240] Standard narrativizations of western philosophy propose an archaic – perhaps primordial – metaphysical option between being and becoming, beneath the theoretical banners of Parmenides or Heraclitus. The dilemma can be formulated in various ways, but its stubborn persistence is an indication of transcendental dialectic (that is, of metaphysical confusion). Heidegger's formulation of critique has direct pertinence here. Attribution of time-characteristics to being is essentially metaphysical. Neither permanence nor impermanence can have application to the transcendental. The reciprocal critical-skeptical question runs: Is time to be found among things? To answer in the affirmative is to sponsor an ontological reduction of time, identified, and taxonomically comprehended, as something that is. (Max Tegmark is among the most important recent thinkers to articulate and defend such a position explicitly.) When cast in the language of commercial practicality, the fissure splits stocks from flows. A decisive option between the two seems in this case unlikely. Complementary duality (of the Chinese philosophical type) is instead suggested.

properties of money were simultaneously abstracted (into ideal qualities) and concretized (through their exemplification in historical monetary media). He writes:

In all countries, however, men seem at last to have been determined by irresistible reasons to give the preference, for this employment, to metals above every other commodity. Metals can not only be kept with as little loss as any other commodity, scarce any thing being less perishable than they are, but they can likewise, without any loss, be divided into any number of parts, as by fusion those parts can easily be reunited again; a quality which no other equally durable commodities possess, and which more than any other quality renders them fit to be the instruments of commerce and circulation.[241]

§5.25 — For Smith, as for Aristotle – and indeed, later, for Marx as for the Austrians – the abstract conception of ideal money was scarcely to be distinguished from the concrete virtues of precious metals (and of gold and silver in particular). Money, insofar as history had certified it, was metallic coinage, only subsequently – and trivially – supplemented by its paper representations, or contractual appendages. Between the questions 'what are the qualities needed by a monetary medium?' and 'why have precious metals been selected to serve as money?' there was only the most insubstantial of differences. To understand why gold made good money was to understand what good money is.[242]

§5.251 — Why, then, do precious metals make good money? The entire list of qualitative monetary virtues can be mined from this question. Due to their chemical characteristics as pure metallic elements, they are durable, divisible, and fungible, since they are stable across time, and homogeneous in space (down to the atomic scale). This substantial consistency also makes them conveniently verifiable, as simple, measurable objects of chemical science, and of practical metallurgical assaying. Finally, but no less importantly, their comparative rarity makes them economically scarce, hence potentially valuable, and – in close proportion to their ratio of value-to-mass – also portable.

§5.252 — Yet, despite its close approximation to the ideal type of a monetary medium, precious metal is not – in itself – money.[243] To become money it has to be minted, or converted into a sign. A concrete

---

[241] See *The Wealth of Nations*, Chapter IV: Of the Origin and Use of Money.

[242] As Edwin Cannan remarks in his introduction to the 1904 edition of The Wealth of Nations, "Values must be measured by some common standard, and this standard must be something generally desired, so that men may be generally willing to take it in exchange. To secure this it should be something portable, divisible without loss, and durable. Gold and silver best fulfill these requirements."

[243] While in particular circumstances, exemplified historically by pioneer societies in frontier gold fields, unminted precious metal can be substituted for money, such employment is most convincingly understood as an atavism. Functionally, it is indistinguishable from the usage of such quasi-monetary 'special commodities' as cigarettes in prisons. As Carl Menger notes in his essay 'On the Origin of Money' (1892), "The peculiar adaptability of the precious metals for purposes of currency and coining was noticed by Aristotle, Xenophon, and Pliny, and to a far greater extent by John Law, Adam Smith and his disciples, who all seek a further explanation of the choice

example is provided by the silver penny, the most widely-accepted monetary unit of the European pre-modern period.[244] The direct descendant of the Roman denarius, dating from 211 BC, the English penny (containing 1.3-1.5 grams of silver) was introduced in AD 785, during the reign of the Mercian King Offa, and persisted with only superficial changes for over nine centuries. It is of particular importance to note that the penny was – to modern eyes – an extraordinarily self-referential sign. What it signified was at the same time what it incarnated. This was captured in the perfect – and to pre-moderns simply tautological – equivalence between the expressions 'one pound is worth 240 silver pennies' and '240 silver pennies weigh one pound'. Silver did not back money, but was rather directly minted into money. The subsequent dissociation of monetary value and precious substance was essentially alien to the pre-modern world. It was only through the debasement of the currency – the archaic monetary manifestation of the DSP – that the difference gained episodic purchase, and then only as a blatant corruption of the currency in question. Coinage is primordially a medium for conveying precious metals into commercial circulation. It shares the economic principle of packaging. In both cases value creation is non-negligible, but also incidental. To see in coining an anticipation of money production of a modern type and scale is thus to entirely misconstrue it. Despite its extreme abstraction, the return of coinage in the mode of crypto-currency is the carrier of a deep conceptual revision, and even a reversion. In its new sense, no less than its old one, a coin is a regular sub-section of an asset-reservoir, sized for commercial convenience, which is to say that it is an actual part of a qualitatively-consistent resource. In neither case does the coin acquire this character simply by saying what it is. Allocation is its irreducible, and non-derivative, semiotic function.

§5.253 — Questions concerning the essential nature of money find themselves slipping backwards, unconsciously and automatically, into a description of the historical instantiation of money, which is a topic dominated – massively – by the function of precious metals within complex societies. It is only

---

made of them as media of exchange, in their special qualifications. Nevertheless it is clear that the choice of the precious metals by law and convention, even if made in consequence of their peculiar adaptability for monetary purposes, presupposes the pragmatic origin of money, and selection of those metals, and that presupposition is unhistorical. Nor do even the theorists above mentioned honestly face the problem that is to be solved, to wit, the explaining how it has come to pass that certain commodities (the precious metals at certain stages of culture) should be promoted amongst the mass of all other commodities, and accepted as the generally acknowledged media of exchange. It is a question concerning not only the origin but also the nature of money and its position in relation to all other commodities."
http://www.monadnock.net/menger/money.html

[244] "By far the most common coin throughout the Middle Ages was the silver penny, known in Latin as the denarius. The word was preserved in the Romance languages as the denier in French, the dinero in Spanish, denari in Italian, and denar in Hungarian. The Germanic languages had their own term: pfennige in German, penningen in Dutch, and pence or penny in English. The coin was typically quite small. Now that you know the term and the coin, you understand why pence in English is abbreviated with a lower-case d, as in: £5 3s 5d."
See: http://europeanhistory.boisestate.edu/latemiddleages/econ/banking.shtml

through appeal to paleo-anthropology, exotic ethnography, or the history of established modernity, that such questions can refer themselves concretely to anything else. Money has been gold, silver, and copper coinage,[245] with only primitive, anomalous, and sophisticated exceptions.

§5.3 — The narrativization of monetary history which has come closest to gaining mainstream acceptance is the evolutionary model of Carl Menger, which describes the emergence of money – or 'indirect exchange' – from out of a primitive barter economy, as a solution to the 'double coincidence of wants'.[246] Menger emphasizes the specific coordination problem involved in transactions by barter, which is the combinatorial explosion of 'direct' (and terminal) exchanges. "These difficulties would have proved absolutely insurmountable obstacles to the progress of traffic," Menger insists,[247] "and at the same time to the production of goods not commanding a regular sale, had there not lain a remedy in the very nature of things, to wit, the different degrees of saleableness (Absatzfähigkeit) of commodities."

§5.31 — Commodities are not equally 'saleable' or commercially disposable, and it is from this diversity that the differentiation of money from the world of commodities takes place. The transitional stage,

---

[245] The hierarchical triad of gold, silver, and copper coinage, while comparatively stable in Europe, has not exhibited a wider consistency across time and space. In China, for instance, gold was not monetized until modern times. Nevertheless, geochemical factors – determining the relative abundance of these metals, among other neatly ordered relevant properties – accounts for its attractiveness as an ideal type (based primarily upon European economic experience). It is conceptually convenient insofar as it places the functions of money as a store of value and a medium of exchange upon a spectrum, corresponding to the metallic order, or scale of value density. Braudel's empirical description elucidates this clearly: "A metal currency consists of a set of related coins: one is worth a tenth, a sixteenth, a twentieth of another, and so on. Usually several metals, precious or otherwise, are employed simultaneously. The West retained three metals: gold, silver and copper, with the inconveniences and advantages of such a mixture. The advantages were that it answered the varied requirements of exchange. Each metal with its coins dealt with a series of transactions. In a system exclusively of gold coins it would be difficult to settle small-scale everyday purchases. On the other hand large-scale payments would present difficulties in a system confined to copper. In fact every metal played its part: gold, reserved for princes, large merchants (even the Church); silver for ordinary transactions; copper naturally for the smallest. Copper was the 'black' money of people of small means and the poor. Mixed with a little silver it blackened quickly and deserved its name." (Vol. I, 458)

[246] In chapter 17 of Human Action, Mises refers to this narrative as: "an irrefutable praxeological theory of the origin of money."

[247] 'On the Origin of Money' (1892): http://www.monadnock.net/menger/money.html
In 'Shelling Out', Szabo integrates the problem into game theory. "Barter requires, in other words, coincidences of supply or skills, preferences, time, and low transaction costs. Its cost increases far faster than the growth in the number of goods traded. Barter certainly works much better than no trade at all, and has been widely practiced. But it is quite limited compared to trade with money. … Money converts the division of labor problem from a prisoner's dilemma into a simple swap."
http://szabo.best.vwh.net/shell.html

within Menger's account, corresponds to the rise of a special commodity, marked out by its peculiar Absatzfähigkeit. The ready acceptance of such intermediate goods within systems of barter exchange, due to their convenience for re-sale – i.e. their liquidity – spontaneously anticipates the monetary function.[248] To re-iterate the kernel of Menger's analysis, at the risk of redundancy: the Absatzfähigkeit of precious metals "is far and away superior to that of all other commodities" (and, compared to this virtue, their traditionally-recognized merits are theoretically relegated to mere "concomitant and subsidiary functions of money"). The genesis of money is thus attributed to a self-organizing process of commercial abstraction, in which liquidity plays the supreme role.

§5.32 — Liquidity cannot be extracted from its commercial context. It translates with great fidelity into acceptability, and thus conceptually converts an extrinsic feature – the degree to which an item of whatever kind encounters general market receptivity – into an intrinsic property. Liquid assets will be readily 'taken off your hands'. They constitute the negative of commercial friction, or resistance, which approaches its minimum in money. ("Everybody needs money. That's why they call it 'money'."[249]) Since markets – whether comparatively concrete or abstract – are nothing but zones of asset liquidization, they tend to convert everything they touch into 'money' at some level of intensity. Anything that can be marketed has a monetary aspect, which is to say that it could – under counter-factual conditions determined by the absence of any superior commercial medium – become money. We return, always, to cigarettes in concentration camps as a reality anchor. Money, fundamentally, consists of market-participation tokens. It need only be swappable. What demotes any such thing, below the threshold of monetary status, is not its own essential deficiency, but always and only better money. It is better money that defines money effectively, while retro-projecting an original idea.[250]

§5.33 — Examples of extreme social relapse – accompanying the destruction of monetary systems through hyperinflation – are regularly invoked in support of Menger's story, because they resuscitate its basic features through regression. When money dies, societies appear to recapitulate its primeval forms – seizing desperately upon candidate 'general commodities' such as cigarettes – on their path of descent back into the dysfunctional tangles of barter relationships. It is especially notable that under

---

[248] For an illuminating discussion of the re-emergence of intermediate goods in the wake of the gold standard, see Nick Szabo's 'Two Malthusian Scares' (2016): http://unenumerated.blogspot.hk/2016/02/two-malthusian-scares.html

[249] This is to repeat the line from David Mamet's Heist that is cited at the start of this book. Beyond the humor, it is perhaps the most insightful contribution to political economy to be found within the history of cinema.

[250] Upon being asked to predict what Bitcoin would ultimately come to be called, Pierre Rochard offered the acute response "Money." The absence of anticipated qualification is, of course, the critical point. Superiority predicts eventual normality. The forecast runs: First Bitcoin, then 'standard crypto-currency', then 'computer money', finally 'money'. Something roughly like this has to be probable, even if the prediction is implicitly revolutionary.

such conditions it is the promissory aspect of money, as credit (corresponding to a liability accepted by another party), that leads the way into worthlessness. Hyperinflation is a catastrophic break-down in trust, when the value attributed to the solemn word of the issuing authority is rapidly re-set towards zero.

§5.34 — The Austrian narrative corresponds to an anti-politics, in which the legitimate domain of concentrated public action is subjected to systematic constriction, in accordance with a radical skepticism regarding both its theoretical sufficiency and its practical efficiency when compared to the history and prospects of spontaneous coordination. Inevitably, therefore, the most significant antagonists of the Austrian orientation are those committed to a defense of politics – one that is equally, and reciprocally, both descriptive and normative. In recent times, the most influential account in this vein has been advanced by David Graeber.[251] The basic tendency of Graeber's historical reconstruction, which folds economics into the politics of debt, makes it emblematic of the anti-liberal philosophy of money in general. It can therefore be taken as exemplary.

§5.341 — Rather than tracing the origins of money back to a process of spontaneous order, in the Austrian fashion, Graeber binds its history to the state. The primordial linkage of money to a 'universal commodity' is de-emphasized relative to its political-economic functions of taxation and debt accountancy. According to this narrative, the principal historical secret of money lies not in the facilitation of trade, but in economic exaction by social elites. Standardization is the essential feature, reflecting – and reinforcing – concentrations of power. The large-scale production presupposed by an oecumenic currency depends upon a monetary manufacturing capacity that can only be provided by royal mints, or their modernized equivalents. Abstraction – or formal mathematization – of the

[251] Graeber's argument is detailed in his work Debt: The First 5,000 Years (2011). The author's academic foundation in anthropology makes it philosophically tempting to categorize his work as an empirical revolt against transcendental – or a prioristic – economic theorizing (of the kind exemplified by Austrian praxeology), and it has been frequently defended on these grounds. Perhaps the most crucial empirical observation, which has already become a staple of anti-liberal monetary theorizing, is the remarkable absence of anything approximating to a 'barter economy' within the record of historical anthropology. The primordial commercial problem, for which money is proposed as solution, has little obvious instantation among human societies – past or present. The pertinence of this apparent fact is irreducibly ambiguous, however, since an economic order based upon barter, even in the terms of the liberal analysis, clearly cannot be conceived as a stable – and thus enduring – social equilibrium. The absence of barter economies from the ethnographic and historical record is thus predictable as a selection effect (with the radical maladaptation of these systems – i.e. their intrinsic inclination towards extinction – exempting them from the domain of empirical evidence). We do not see them because they do not work. For a succinct Austrian riposte to Graeber's theory of monetary history (along these lines), see Robert P. Murphy's 'Origin of the Specie' http://www.theamericanconservative.com/articles/origin-of-the-specie/

primitive social obligations within what Graeber dubs "human economies" leads to a radical intensification of oppression and violence.

§5.342 — The axis within which Graeber's analysis unfolds is determined not by (commodity) trade, but by obligations, stretching from the fluid reciprocities of primitive societies – and residual "everyday communism"[252] – to the cyclopean power structures of centralized states. Within the latter, as recorded already in the excavated tablets of ancient Sumer (c. 3,500 BC), cash money has been consistently marginalized relative to financial credit. It is this construction that supports Graeber's inverted sequence of monetary history, which is no longer conceived as an abstraction from commercial traffic, but instead as a commercialization of formalized obligations, beginning with credit as the primordial phenomenon. It is from debt that money is subsequently developed, with barter appended, at the end of the theoretical sequence, as a mutant, terminal annex. Credit and not barter, then, or obligation and not trade. This is, for Graeber, the political matrix in which money is born. An innovation in social hierarchy is its midwife, introducing it to the world through the "military-coinage-slave" complex of the Axial Age civilizations.

§5.343 — It is notable that Graeber considers the Axial Age[253] to be an essentially unmitigated historical calamity. Where Karl Jaspers drew attention to an incomparable cultural awakening,

---

[252] Graeber's fascination with the entanglement of debt and definite moral ideas is overtly indebted to Nietzsche's On the Genealogy of Morals, down to the details of its etymological observations. In particular, the moral-economic ambivalence of Schuld (guilt / debt) is crucial to both. It can be predicted with some confidence that this Nietzsche text – untimely in a way that is only now becoming starkly apparent – is set to acquire a special prominence among the emerging conditions of the 21st century, as the foundations of contractuality are subsumed into the technosphere, and thus require explicit formulation.

[253] Karl Jaspers coined the term 'Axial Age' (Achsenzeit) in his work The Origin and Goal of History (Vom Ursprung und Ziel der Geschichte, 1949). Thinkers of the Axial Age include Laozi (Lao Tse, 6th-4th century BC); Kongzi (Confucius, 551–479 BC); Li Kui (455-395 BC); Mozi (470–c.391 BC); Yang Zhu (440–360 BC); Mahavira (599–527 BC); Gautama Buddha (c.563-483 BC); the authors of the Upanishads (from 6th century BC); Thales (of Miletus, c.624–546 BC); Anaximenes (of Miletus, 585-528 BC); Pythagoras (of Samos, c.570–495 BC); Heraclitus (of Ephesus c.535–475 BC); Aeschylus (c.525-455 BC); Anaxagoras (c.510–428 BC); Parmenides (of Elea, early 5th century BC); Socrates (c.469–399 BC); Thucydides (c.460–395 BC); and Democritus (c.460–370 BC), among others. The origination of philosophy in this historical episode is scarcely deniable. The Neo-Marxist explanation, re-animated by Matteo Pasquinelli, is rooted in the work of Alfred Sohn-Rethel and the identification of real abstraction. Philosophy is located downstream of a distributed cognitive machine, activated by the creation of money.

http://onlineopen.org/capital-thinks-too

Our question 'what can money do?' is thus modulated by the compelling hypothesis that to be included among the things money has already done is the initiation of philosophy. According to this understanding, 'philosophy'

occurring in the centuries around the middle of the first millennium BC, Graeber derives its efflorescence from a revolutionary advance in the machinery of social oppression. The ascription of values is reversed. Yet abstraction is the consistent key to both accounts. Concrete existence becomes calculable on an unprecedented scale. Something like a 'question of being' arises. Graeber earns his role in this discussion through participation in the hypothesis that monetary innovation – operating as a spontaneous stimulus to abstract thinking in general – is the basic phenomenon. During the Axial Age the world begins to learn what money can do.

§5.344 — Graeber's analysis is consistent with a far wider cultural tendency to conceive debt as the principal instance of economic domination (supplanting the classical role of mere destitution in this role).[254] Social contestation over economic flow (profits versus wages) is displaced by a central image of class war between creditors and debtors, radically and fundamentally financialized. This is not a socio-historical construction to be lightly dismissed. The model of political revolution as an insurrectionary extinction of debt, in particular, is productively suggestive. It embeds into itself a theory of post-revolutionary social memory – or strategic amnesia – in obvious accordance with large swathes of historical evidence. The revolutionary 'Year Zero' symbolically wipes the slate clean. Evidently, the financialization of capital and its revolutionary negation have modernized in parallel, if not at tightly-bound velocities.

§5.3441 — While the complex historical entanglement of modern revolutionary politics and ancient eschatalogical religion is a well-worked topic far exceeding the scope of this book, it intrudes inescapably at this point, in the specific guise of the jubilee.[255] 'Redemption' is a term cutting across

– defined so broadly that it comprehends even the birth of systematic mathematics (Euclid) – is a side-product of social monetization. Its cognitive machinery cannot be accurately specified at any level that falls short of commercial process. The conceptual equation does not precede the exchange relation. In the beginning was the swap.

[254] A Malthusian lineage passing through David Ricardo's Iron Law of Wages made the primary contribution to the classical Marxian analysis. The identification of a socio-historically contingent 'natural' or equilibrium tendency for wages to approximate to a subsistence income, under conditions of chronic labor supply glut, was the prediction that propelled the Marxist analysis to its peak of popularity – at least in the West – during the late 19th century epoch of mass proletarianization. It can surely be no coincidence that the recession of this paleo-Marxist immiseration thesis – among conditions of comparative generalized abundance – have been accompanied by a redirection of critical attention from the commoditization of labor to the registration of accounts, associating economic oppression with debt peonage, rather than absolute destitution.

[255] The Jubilee (yovel), referenced already in the Torah (or Pentateuch), is the culmination of a – seven-times-seven – 49-year meta-cycle, in which 'the slate is wiped clean' by debt-forgiveness. Every seventh year of the ancient Hebrew calendar was a shemita or fallow year, of which the Jubilee is evidently an extrapolation. (The modulus-seven pattern is generally accepted by scholars based upon overwhelming evidence, notwithstanding the description of the Jubilee in Leviticus 25:10 as the 'fiftieth year'.) Within the cyclic system of the jubilee, debt-

the registers of religious and economic discourse, sustained by a consistent appeal for absolution, or forgiveness. From Prophetic Judaism to Graeber's Debt: The First 5,000 Years, via The Merchant of Venice, Das Kapital, and countless additional examples of anti-usurious polemic, the voice of the debtor has been bound to an apocalyptic promise of forgetting. The obliteration of the secular ledger in the name of a higher accountancy has been the insistent theme. For roughly a century, administrative inflation-tolerance has provided a moderated expression for the same popular clamor. Inflation strikes a compromise with the demand for financial tabula rasa, by erasing debt values incrementally. It is revolutionary redistribution on an installment plan. The veil of the ubiquitous credit system allows inflationary macroeconomics to reach beyond debt, and make the abominated 'liquidity preference' of cash accumulators its target. Money as a 'store of value' – as economic memory – is brought into the arena of programmatic erosion. In this way a chronic, or normalized, war on money offers a concession to populism that epitomizes the compromise-formation political economy has become. Socialist revolution is forestalled by a continuous debauching of financial signs, but in this way it is also executed. Macroeconomics delivers eschatological communism in slow motion. An explicit attraction of discretion-protected crypto-currency is making such deals unobtainable.[256]

§5.345 — Initially at issue here is the sanctity (or sacrilege) of the free contract – an essential pillar of the liberal social order from the perspective of the right, an objectively-merciless formalistic extravagance from that of the left. Supporting these contrary judgments are diverse ethnographic orientations inclined, respectively, to the naturalization or denaturalization of commercial life (with Smith's "propensity to truck, barter, and exchange one thing for another" See: The Wealth Of Nations, Book I Chapter 2 at one end of the spectrum, and Graeber's "everyday communism" at the other). Providing consoling doctrines, respectively, to the 'haves and have-nots', this axis of variation reflects

---

annihilation appears as an equilibrium function. The regenerative (positive-feedback) tendency of money as proto-capital is capped by a circuit-breaker. From the perspective of human social conservatism, there is no doubt a perennial wisdom in this, even if it runs directly contrary to the trend of the modern (Ashkenazi) contribution to finance capital in its attainment of historical escape velocity. Any deeper venture into the ironies of Jewish socio-economic history exceeds the ambitions of the present work.

[256] Absolution is the theological model of the reversible commitment, and thus of time annihilation. Time cannot forgive, by definition. It is non-retraction in-itself. Only within a soteriological construction of eternity can what is done be undone. To be saved is to be rescued from the intrinsic consequences of time. Can there be serious doubt that the project of reversing the irreversible provides the final content of modern political dialectics, and especially of 'revolution' in its dominant modern sense as applied soteriology? Aufhebung is absolution, undisguisedly. The transmission mechanism, from theology to political history, is provided by the Nietzschean insight (from On the Genealogy of Morals) that institutional slavery has a humanistic origin, offering immediate respite from execution, and mediate opportunity for redemption, to a defeated enemy. In this context, deferred settlement is mere contingent survival, or mercy in the form of time. Primordially, the condition of slavery is a stay of execution. One owes everything to the hesitation of the killer, within which a transition from military history to economic history surreptitiously takes place. Debt peonage is the bridge.

an antagonism no less durable than the human species itself (and quite possibly more enduring by far). There is a liberal and a socialist End of History, and neither unambiguously approaches. This is what any social animal – poised between the tiger and the mole-rat – should expect. Persistence of ideo-political conflict is the safe prediction, with the corollary that partially-insecure property is the socio-economic norm. Projects to strengthen or weaken property security – that is to adjust its degree of political insulation – mark the PPD like traffic indicators, illuminating its basic axis, and describing the great games.

§5.35 — Without seeking to wholly efface the novelty of Graeber's construction – still less its remarkable pertinence to our contemporary political-economic concerns – it is important to note the extent to which its theoretical stance is prefigured in crucial respects by the German Historical School of economics,[257] and thus, in turn, anticipated in considerable detail by the Austrian thinkers. Menger, in particular, defines his enterprise in explicit contra-distinction to those who place the State at the origin of the monetary phenomenon, which he conceives as the dominant economic error of his time. Since a functional unit of account already presupposes a prior settlement of the value question, through a process of price discovery, Menger confidently maintains that:

It is not impossible for media of exchange, serving as they do the commonweal in the most emphatic sense of the word, to be instituted also by way of legislation, like other social institutions. But this is neither the only, nor the primary mode in which money has taken its origin. … Putting aside assumptions which are historically unsound, we can only come fully to understand the origin of money by learning to view the establishment of the social procedure, with which we are dealing, as the spontaneous outcome, the unpremeditated resultant, of particular, individual efforts of the members

[257] The German historical school of economics was essentially characterized by its aversion to universal mathematical-equilibrium models, of the English classical and neoclassical type. Empirical peculiarity, as carried by the details of social history, was promoted against highly-generalized cross-cultural constructions. In this respect, it was a recognizable descendent of the German Romantic tradition. Its most prominent representatives included Wilhelm Roscher (1817-1894), Bruno Hildebrand (1812-1878), and Karl Knies (1821-1898). The distinctive characteristic of this school is its consistent attempt to delimit classical models within a more complex socio-historical matrix. When translated into the Anglophone world, the principal concerns of the German historical school are perhaps best represented by the New Institutional Economics, developed from the work of Ronald Coase, most notably by Douglass North. Yet here one sees a fundamental distinction in methodical orientation, indicative of broader cultural difference. Among the Coaseans, the principle of intelligibility for an economically-significant institution remains grounded in commercial coordination. Transactional economy explains the existence of an institution (and first of all, the firm). The market process is abstracted, rather than theoretically subordinated. Historical institutions that appear super-economic under German inspection are configured instead as meta-economic by the later Anglophone analysis, which generalizes microeconomics beyond its neoclassical frame.

of a society, who have little by little worked their way to a discrimination of the different degrees of saleableness in commodities.[258]

§5.36 — Despite their strategic mismatch, or ideological divergence, the motivated narratives of Menger and Graeber nevertheless converge upon a precise conception of the stakes in theoretical play. For both, there is an application of historical story-telling to a liberal theory of money, seen as essentially bound to the status of precious metal coins. That Menger writes in defense of this theory, and Graeber in opposition to it, does not affect the invariable associative core in the least. Both agree entirely about what it is that the valorization or denigration of money – as minted metal – means. Far too much socio-historical ballast underlies this construction of the controversy to allow for its casual dismissal.

§5.4 — The controversy is significantly deepened by a third narrativization of monetary history, outlined in Nick Szabo's remarkable essay 'Shelling Out'.[259] Szabo extends the investigation into the origin of money far back into prehistory, where it hazes out into evolutionary time. The essay takes as its initial clue a peculiar pattern of linguistic interference between money and marine molluscs, as evidenced in the "shelling out" of the title, and in the persistent colloquial naming of dollars as "clams".[260] The source of this association is found in the 'wampum' shell-money of the native tribes encountered by mid-17th century New England colonists, which provided the settlers with their first "liquid medium of exchange" and subsequently their first legal tender (from the period 1637-1661). The opportunistic shell currency of the New England colonists finds numerous ethnographic echoes up to present times, and dating back into the deep Paleolithic, 75,000 years ago. Szabo categorizes such shell currencies among 'collectibles', noting that such types of 'proto-money' or 'primitive money' were "the first secure forms of embodied value very different from concrete utility". Recognizably, they were a response to the problem of 'value measurement' (with no profound distinction required between 'goods' and 'obligations'[261]) facilitating the crucial innovation of delayed reciprocity.

---

[258] Accessible online at: http://www.monadnock.net/menger/money.html

[259] The intensity of Szabo's involvement in the crypto-current would make his contribution to the general theory of money singularly pertinent, even were its theoretical quality less outstanding. See: 'Shelling Out – The Origins of Money' (2002) http://szabo.best.vwh.net/shell.html

[260] Notably, the association between shells and commerce has been promoted by the name of Royal Dutch Shell (familiar to Americans through its subsidiary the Shell Oil Company). The 'Shell' Transport and Trading Company (quote marks were included in the title), founded in 1897, was the British side of a merger (in 1907) with the Royal Dutch Petroleum Company that created the international oil giant which still exists today. The pre-merger 'Shell' did indeed derive its name from traded sea shells, although this was the main business line of a predecessor company, whose identity was adopted, rather than a continuing commercial specialism. Sadly, shell-trading in the Dutch East Indies does not seem to have been central to the emerging global oil industry.

[261] Given the biological centrality of food sharing among social animals, it is peculiar that the difference between the recognition of an obligation and the receipt of a commodity could ever be considered of primordial

Systematized exchange serves as a proxy for resource storage. "Like fat itself," he writes, "collectibles can provide insurance against food shortages." The hook they offer to consolidation through natural selective is therefore considerable.

§5.41 — Compared to Homo neanderthalenis, Homo sapiens was Homo economicus. This was a species that carved out a competitive advantage for itself relative to other hominids of similar – or even superior – individual intelligence through the partial commercialization of its environment. A distinctive genetic endowment, expressed through attachment to collectibles, enabled spontaneously-coordinated social action to arise with unprecedented sophistication. By providing – for the first time – effective incentives for activities oriented to regular exchange, collectibles normalized trading as a quasi-continuous, characteristic human behavior. Social existence acquired a commercial dimension, with corresponding stimulus to cognitive advancement beyond the horizon of immediate utility.

§5.42 — Time was not only the medium of change, as this was accumulated through adaptive genetic modification of hominid species, but also its driver, or prompt. More specifically, modern man's prehistoric ancestors were compelled to adapt to the concrete irregularity of time.[262] Seasonal variation

---

importance. The distinction becomes discernible only through formalization, which corresponds to economic engagement with strangers (marking the phase-transition from anthropology to sociology). When precipitated from the dense fabric of tacit reciprocities, trade accelerates settlement. The game-theoretic structure is comparable to a collapse into non-reiterating interactions, with associated attenuation of reputational structures. Under such circumstances, the importance of compact, instantly-completable, or fully-executable transactions is elevated. Anything left unfinished is potentially lost. Money, in its positive sense (as collectible), thus emerges as an anti-memory. The subsequent elaboration of formal credit systems only emphasizes this fact, insofar as unsettled obligations are priced as risk, and thus exposed in their definite disutility. Graeber's emphasis upon 'everyday communism' is especially unhelpful within this deep context, insofar as it merely assumes the solution to a collective action problem – presenting it as an irreducible ethnographic fact. Parochial inattention to the complexities of trade is promoted as a positive ethical achievement. The question posed by evolutionary biology, which is no different to that of realistic social analysis, is subjected to blank dismissal. Given the considerable (positive sum) advantages of sharing, and the evident coordination problem obstructing it, how is reciprocal altruism actually possible? Markets, concretely, answer this question. Insofar as it can be obliterated in theory, they too can be. This only demonstrates how far theory can depart from realistic application, without losing – and perhaps even enhancing – its function as political rhetoric.

[262] The transcendental-philosophical problem of time production is approached here as a topic of evolutionary anthropology. Time is distinguished from the present moment through contextualization of present conditions within a larger time-frame. In this way, the cognitive integration of time is the exact complement of its commercial disintegration. For a-synchronous transactions to meet a criterion of reciprocity, they require a mechanism that supports – or effectively substitutes for – deferred settlement. This is a notion comparable to the 'time-binding' explored in Alfred Korzybski's general semantics. The human capability for deterritorialization or comparative environmental independence in space is both echoed and advanced by a capacity for expansive time colonization, with proto-money operating as a cognitive condenser. An inheritable token with the potential to support future acquisitions explodes economic immediacy, in both directions. Its value is inseparable from a time-integration

compels rudimentary specialization. Outside tropical latitudes, it was simply impossible for primitive man to engage in a consistent pattern of activities across time. Food sources were not constant – or even continuously available – throughout the annual cycle. Winter, in particular, set its own challenging demands, which could be met only by running down food stocks (provisions). Hunting large herbivores accentuated these conditions of episodic glut, and the corresponding need to organize time. The template for division of labor and trade was therefore already laid by climatic adaptation, prior to any significant extension across space, and into elaborate social specialization. Economic incentives had necessarily to be scaled beyond immediate needs. (Much space for differential anthropology is opened here.)

§5.43 — At the level of maximum abstraction, money – already in its most primitive instantiation – enables the commercial disintegration of time. This is captured at the level of hominid ethology by the facilitation of delayed reciprocity. (It is only through pedantry that 'reciprocal altruism' can be significantly differentiated from 'trade', abstractly conceived.) Monetized trade tolerates de-synchronization. Accumulation of collectibles within a circuit of exchange is equivalent to a transactional non-simultaneity – complementary to a primitive 'borrowing' of the specific good in question[263]– which allows for the commercial exploitation (arbitrage) of variation in time-preference over an asset. To repeat the critical point: Money – already in its most primitive inception – formalizes time-disintegrated reciprocal altruism, by providing the condition for its simultaneity. The receipt of money now substitutes for the persistence of a debt.

§5.44 — Szabo's analysis returned money to the comparatively neglected semiotic function of collection, or allocation, within which value exchange (circulation) and storage (accumulation) find a common root. Collected signs are irreducible to signifiers and indices. Their value is not soluble within semantics. The economic category of scarcity is essential to them. It is only in collection that the

---

function, which can equally be conceived as a tolerance for time-disintegration, or de-synchronization. It is the virtual suture, permitting the opening of a time-rift. The sheared edges connect only through it. Money lets time-consciousness fall apart. When regressed to the level of the collectible, 'money' designates a critical threshold in evolutionary psychology. It is money – even more than 'the tool' – that differentiates man from alternative hominid lineages. Homo economicus, then, is at once a modern telic construction, and an archaic cladistic marker. The monetarization of social obligations has consequences that are not restricted to the time-horizon of the psychological individual. Money facilitates the accumulation of inheritable wealth, enabling inter-generational resource transfers, in accordance with incentives strongly predicted by any biorealist account of kin altruism. It thus opens the conceptual space for transferable non-consumption goods, distinct from either territory or perishables. 'Wealth' becomes dynastically assignable, thus achieving a comparative independence from primitive power (or immediate dominance).

[263] The theoretically erroneous translation of this flexible exchange into a credit relation will concern us presently.

'economy' of signs ceases to be a metaphor. Collectible value tokens cannot be loaded from a dictionary. They have to be economically acquired.

§5.45 — It might easily seem, under conditions obscured by the creditization and politicization of money, that collectibles are – from the moment of their inception – a prototypical mode of saving (and therefore – by iron reciprocity – of debt). It cannot be sufficiently emphasized that this path of interpretation is profoundly erroneous. This is a point that merits explicit comment precisely on account of its elusiveness, which reflects structural factors of great historical consequence. Money, whether in Menger's sense, or in Szabo's – and even in Graeber's, once allowance is made for his historical inversion of the credit-money relationship – extinguishes debt. Any monetary transaction substitutes for the persistence of a liability. Acceptance of primordial or non-credit money, whether in the form of a 'collectible' or (more specifically) of a precious metal coin, is the alternative to persistence of a credit position. In such cases, receipt of money erases an obligation, rather than confirming, memorizing, or reproducing one. Historically, at least, 'paper' or credit money is the anomaly. It is only in this case that monetary assets correspond to another party's debt, that is, to a preserved obligation. Monetary exchange does not intrinsically involve a credit-debt structure, prior to its financialization. It appears to imply such a structure only when the reality of money as a (comparatively abstract) positive asset has been dissolved, until it appears as no more than a surface effect, or epiphenomenon, of its registration within the ledgers of a banking system. Debt is the conceptually and institutionally convenient interpretation of a more obscure social phenomenon. Market acceptance of money is systematically reconstructed into the recognition of an obligation, as if it exhibited dependence upon an implicit contract. The conceptual imperative at work here is gregarious. Its orientation is to socialization.[264] The tendency is to obliterate all trace of an asset that isn't already a recording of debt. Liquidity is reconfigured as an entitlement.

---

[264] One highly-influential dynamic model of value socialization – yet to reach its apogee of cultural influence – is found in the work of René Girard. The basic theoretical matrix is laid-out in his (1972) book Violence and the Sacred. It is a notable merit of Girard's work that rather than merely assuming the social diffusion of values, the process is at least partially explained, albeit through the employment of various relatively cumbersome (or metaphysically-saturated) axioms. In particular – and understandably – theory of mind is presumed solved, and operative as an engine of gregariousness. Girard's guiding proposal is that desire is mimetic, which is to say social and antagonistic. Its template is always the desire of the other. Concupiscence is originally envious. I'm having what he's having. Libidinal privacy is thereby rendered inconceivable, with human desire being collectivized ab initio, on a basis essentially incommensurable with the instincts of a solitary animal. It follows that the more anything is wanted, the more it is wanted. Desire spreads through the social body like a contagion. The extreme reflexivity of any system that can be modeled this way makes it explosively excitable, with a tendency towards some crescendo of violence (or 'sacrificial event'), through which explosively accumulated mimetic tension is discharged. In recent years, the translation of Girard's model into a more colloquial economic register has been undertaken by Peter Thiel. Mimetic desire is identified with economic competition.

§5.46 — Employment of a single word – 'money' – for these very different types of valuables lends itself to systematic theoretical disorder. The depth of this confusion is indicated by the fact that not only 'money', but also 'assets', and even 'cash' have been progressively assimilated to the concept of credit[265], in accordance with a general financialization of economic categories that has been consolidated – at an accelerating pace – over recent centuries. Since the concept of money tends to accommodate itself to the dominant pattern of actual monetary usage, it has increasingly been identified with a positive financial balance in a bank account, recorded in the bank's ledger (where it is registered as an institutional liability), and even – beyond this – with the notion of a credit limit determining spending power. Money has come to seem increasingly like something banks do, through trusted record-keeping fundamentally. On this track it tends to become the name for a complex of banking services.

§5.47 — In order to control these semantic instabilities, it is worth provisionally introducing – in lieu of enduring technical terminology – a distinction between A-money and C-money.[266] 'A-money' is a positive asset, or collectible, uncorrelated to a liability. In the case of Bitcoin, it consists of DSP-proof (or non-duplicitous) ledger entries. The value of A-money is not in any strong sense 'intrinsic' but depends – as all commercial value does – on market receptivity. It varies, therefore, between zero and some arbitrary magnitude, when denominated in any other medium whatsoever. This variance, however, has no element of credit risk (or sensitivity to default). No one is under an obligation to redeem A-money for anything. Like any other collectible, it has value in anticipation of market

---

[265] 'Credit' and 'credentials' are roughly the same word. Both of its branches pass into English (via Middle French) from the Old Italian credito, vernacular modernization of the Latin creditum, meaning something entrusted, a loan, from the neuter of creditus, past participle of credere to believe, entrust, source also of creed and credence. Credit and trust are indissociable conceptions. It is not only that etymological sense continues to operate within contemporary ordinary usage. Under the current techno-cultural pressure of monetary sophistication, it is undergoing re-activation. Money cannot be technically understood, it turns out, without the concept of trust undergoing complementary rigorization. Economic convulsion corresponds to a crisis of belief.
According to the dominant (if tacit) teleological scheme, monetary evolution advances along a path of credit elaboration. It trends therefore to financial domination by sophisticated derivatives ('contingent claims') composed of options, forwards, and swaps. The sequence of tradable financial products commercializes risk at ever higher levels of distillation. It advances from positive assets, to liabilities, to formalized trading options under specifically-contracted time and price conditions. Credit therefore strongly aligns with financial teleology. It is in an important respect owed the future. The trouble Bitcoin introduces to this structure of meta-debt cannot, therefore, be anything other than considerable.

[266] The term 'C-money' has been selected to avoid confusion with Wei Dai's 'b-money' concept (whose importance to the genesis of Bitcoin is beyond controversy). Simple alphabetical order has otherwise been adhered to. Any apparent resonance between the 'A-' and 'C-' of these provisional terms and the distinction between 'asset-' and 'credit-money' is purely serendipitous.

acceptance, and not on the 'basis' of any promise made by an issuing authority. It is a commodity, in the broad sense. Redemption is intrinsic (or immanent) to it.

§5.48 — C-money, in drastic contrast, is credit (corresponding to the obligation of another party). It has no value at all separable from the credit quality of the individual or – far more typically – institution that has registered its issuance as a liability. If a depositary accepts A-money for safe-keeping, and thus 'on loan', the signed receipts it provides to guarantee restoration of the funds in question are already germinal C-money. This was, as a matter of historical fact, the transactional mechanism that catalyzed modern monetary transformation, from precious metal coinage, to promissory notes, and eventually to credit accounts. The value of C-money is based upon institutional guarantees. Trust is a mathematical coefficient of its value. Trustlessness is therefore essentially intolerable to it. At trust degree-0 C-money necessarily becomes worthless. In each such case, as a matter of historical factuality, an episode of hyper-inflation would then have consummated itself. This is how (C-)money dies.[267]

§5.49 — Evidently, Bitcoin is a variety of A-money, and not a C-money (or credit) system. Its currency units do not index obligations. They are positive abstract assets. As Szabo insightfully concludes, Bitcoin is a system of digital collectibles. While it is certainly possible to be owed bitcoins (like any other asset), in owning bitcoins one is not thereby owed anything further. The application of the credit relation to bitcoins has necessarily to draw upon institutional resources extraneous to the Bitcoin protocol itself. Crypto-currencies perfectly simulate precious metals in this respect. No promise is inherently attached to them. They can be the substance of wagers, but they are not bets on the word of another agent.

§5.5 — Conceptual conversion of A-money into C-money has been an automatic outcome of modern financial history. It can formally, but only artificially, be disentangled from the development of banking procedures and institutions. The credit (or reputation) of the financial institution supplants the positive asset value of money, as it replaces the monetary commodity with authorized notes. This financial reconstruction of exchange introduces an element of non-simultaneity. A moment of indebtedness is inserted into the synchronous swap, a period – however fleeting and notional – in which payment is owed. Even a simple purchase can be formally elaborated in this fashion. Payment need only be preceded by a ghostly double – a liability – arising in the non-instantaneous space of commercial reciprocity. A pseudo-consecutive schema insinuates credit into exchange. It is only on the basis of a systematic social hallucination of a decidedly metaphysical type, however, that it can be considered always, necessarily, to have been there.

---

[267] The reference is to Adam Fergusson's classic study of Weimar-era hyper-inflation: http://store.mises.org/When-Money-Dies-P10438.aspx

§5.51 — Credit money, then, presupposes a suppression of simultaneity. We are returned to generalized spacetime, although now on the other side. If arithmetic is the formalization of time, in accordance with the Kantian understanding, simultaneity translates to zero. It is the temporal determination of space (or the pure form of non-separation in time). Events occur simultaneously when no time separates them. Under such circumstances, the credit relation is impossible. The critique of monetary financialization is thus bound to the philosophical – and even, by strong analogy, cosmo-physical – problem of simultaneity. If the very notion of the same time, in its global application, is judged irredeemably delusory, then the financial model of transaction is vindicated, as a universal truth. Relativity and fundamentalist credit finance share a metaphysics, in which the absolute occurrence of instantaneous transactions is de-realized, and subordinated in principle to qualification, or mediation. "Simultaneity is a convention," Poincaré insisted. The subsequent relativistic revolution in physics has trained readers to invest this statement with a maximum of intrinsic skepticism, as if it amounted to the claim that simultaneity could not – in principle – ever be actually realized, unless as a standing social illusion.[268] The inversion is then total. Since it is the function of (positive) money to restore simultaneity, the very possibility of any such non-credit currency is in this way dismissed. Hard money contradicts generalized financial relativity, and that has become our common sense. A return of hard money, as anything beyond a relic, can only be manifested as an alien invasion.

§5.52 — Transcendental aesthetic is exhausted by the blockchain. In restoring absolute time (pure succession), Bitcoin recovers simultaneity at the same time. The term blockchain already tacitly says as much. The block is a chunked unit of simultaneity, just as the chain is an order of succession. Each is reciprocally determined by the other, despite their real difference. Critically, a block is validated as a whole, at once. It contains no internal temporal articulation. Each block is all space, in the temporal sense, or non-decomposable duration. It is a true moment, or a 'now', even when sedimented (chained) into the past. Transactional simultaneity is thus realized. As we have seen, this is the negative of

[268] A 'standing social illusion' or "consensual hallucination" – to draw upon William Gibson's anticipatory description of Cyberspace – can, under certain very definite circumstances, attain robust virtual reality in the epoch of the Internet. It can, in other words, be effectively installed. Any residual associations with mere mass delusion, of a kind vulnerable to destructive reality testing, then become systematically misleading, as the index of a misapplied empiricism. The protocol is not an error awaiting correction, but rather a structure of transcendental subjectivity. Its relation to objects is not representational, but productive. The fatal emergence of time as synthetic being, in particular, manifests the techno-historical restoration of transcendental philosophy. The order of things has to be produced. In this vein it has to be argued that the artificiality of time is – finally – time's most time-like quality. Its nature is to be unnatural, at least in the sense that it eludes all prospect of objectification. Only thus does it secure itself against the geometrical reduction that would collapse it into space. Of course, if not obviously, nature itself does this first. To repeat what can never be repeated sufficiently, Φύσις κρύπτεσθαι φιλεῖ ("Nature inclines to crypto.").

financialization, and its actual condition of impossibility. The credit relation has no reality on the blockchain, even though all of its associated signs can be recomposed there.[269]

§5.53 — Profound historical tendencies ensure that this point will be misunderstood, even as it stubbornly – and with at least equal necessity – re-asserts itself. Bitcoins are not credits. Furthermore, and still more controversially, none of the items of economically-significant information embedded within the blockchain are, or could be, credits, unless from a perspective, which is also to say an apparatus, that transcends the blockchain. The temporality of the 'block' ensures this. Nothing unsettled survives the automatic editing process. Only positive signs persist.

§5.531 — Consider a simple safety deposit box. It physically and institutionally protects anything placed inside it. 'Intrinsically' precious items (collectibles) are the neatest examples – gold or silver coins, jewels, antiques, or works of art. As with the blockchain, however, complex semiotic objects – such as contracts of any kind – can also be safely deposited. The critical question now arises. Does this mean that such a secure storage facility protects promises to pay?

§5.532 — The answer is not entirely straightforward, since it depends upon the obscure undercurrent of the question. What does it mean to keep a promise? If all that is required is to remember it, then safety deposit boxes can certainly help – and the blockchain vastly more so. If it is further required that the promise be fulfilled, or settled, what is demanded is the time-sensitive elimination of a discretionary factor. In keeping a promise, a tacit betrayal option is cancelled. This is not something a secure deposit, or blockchain, can maintain, because neither is able to hold such an option open.[270] Potential defection ('default') does not require risk-pricing in such an environment, because it cannot occur. Whatever risks there may be to Bitcoin transactions, this is not among them. On the blockchain, no difference between a 'deposit' and an 'account balance' can exist. Credit risk is necessarily zero. There are no negative balances, but only positive holdings, recorded as a history of mining events and

---

[269]The blockchain is thus something like an anti-structure, occupied only by positive terms.

[270] If double spending were a practical option which as a matter of discretion was not executed, then a promise would have been kept. In this case, a credit relation would have been supported. In respect to Bitcoin the example is, of course, entirely counter-factual, and actually logically unconstructible. A double spending tolerant ledger could not be a blockchain, by elementary definition. As Pierre Rochard notes in his short essay on 'The Bitcoin Central Bank's Perfect Monetary Policy', Bitcoin precludes the re-emergence of fractional reserve banking within its medium by automatically necessitating "full reserves for all accounts". The protocol interprets any process of money multiplication as double spending, and edits it out of the economy. Because bitcoin are not credits, "money is not destroyed when bank debts are repaid". The 'money supply' – in the Bitcoin epoch – is constituted by a reservoir of positive abstract assets. Rochard predicts that "The Bitcoin Central Bank [i.e. the decentralized Bitcoin Network] will be the longest lasting institution of its kind thanks to the anti-fragile independent monetary policy it has set in stone."
http://nakamotoinstitute.org/mempool/the-bitcoin-central-banks-perfect-monetary-policy/

transactions. Anything running on a blockchain inherits this characteristic. Smart contracts, for instance, insofar as they are fully-immanent to the blockchain, cannot be credit instruments. They are, instead, hard commitments. The future is effectively pulled forward, and metalized as destiny. (This is a point to be more adequately engaged shortly.)

§5.54 — When attempting to grasp what, through Bitcoin, money ceases to be, the relationship between credit money and fiat currency merits particular attention. This relation is certainly not simply analytical, despite the intimate historical connection between monetary financialization and politicization.[271] Over the course of recent centuries, the problem of trust – as dramatized by episodic banking crises – has functioned as a relay. As previously noted,[272] the spontaneous evolution of paper money (from warehouse receipts) profoundly exacerbates the double spending problem. Considered as the most economically intimate field of media development, it subsumes forgery into printing, on a path that leads to electronic digitization. Within the modern history of money, however, this semiotic main-current is a side-stream. Deliberate fraudulence, involving cynical fake-money production, has not been the principal trust problem generated by financialization. Credit creation, through fractional reserve banking, has been vastly more consequential as an engine of trust catastrophe, precisely because it separates the question of trust from suspicion of criminality, and thus from the sphere of traditional law-enforcement mechanisms. A banking crisis is not – unless contingently, or under the aspect of polemical extravagance – a crime. More generally, those socio-cultural forces disposed to consider inflationism in all of its aspects as essentially criminal have been so thoroughly defeated that their objections have lost all engagement with effective mechanisms of legal enforcement.[273]

---

[271] Conceived in Marxian terms, this history seems to tell of the death of the liberal economic order through its own excesses. Such a narrative is very far from straightforwardly misconceived. The very idea of a liberal regime suggests extreme paradox, precisely because it corresponds to an exemplary coordination problem. The overall order presupposes a suppression of defection which it is itself seemingly unable to guarantee. The 'itself' here – as in all cases of spontaneous order – is the crux of the conundrum. The system of competition itself, or as such, has no obvious allies. Many, if not all, of Marx's classic capital contradictions are rooted in this dilemma (and thus describe a variety of fundamental liberal coordination problems, socio-historically expressed at varying degrees of elaboration). 'The market' – to thus name society's most fundamental spontaneous institution – is susceptible to the ravages of an agent-principal problem without comparison. The attempt to operationalize the state as the relevant agent in this situation, tasked with responsibility for managing general commercial conditions, broadly coincides with the tragedy of modernity, as distilled into 'neoliberalism'. Public Choice theory arose as its more-or-less explicit rejoinder.

[272] See §3.06.

[273] There is no one who can be sued for the destruction of the US Dollar (by more than 95% of its value) over the course of the 20th Century, for instance. Still more extreme – hyperinflationary – depredations enjoy sovereign immunity against legal redress. To decry this situation as itself manifestly criminal is merely to court intensified marginalization. Such has been the libertarian road.

§5.55 — To recapitulate the discussion from Chapter Three (§3.06), when fractional reserve banking turns bad, it is exhibited as a double – and in fact multiple – lending problem. Any bank deposit can be loaned out multiple times, with the proportions of potential bank credit to assumed liability decided by the reserve ratio. (A reserve ratio set to cover 10% of loans outstanding permits a ten-fold credit multiplication effect, prior to inter-bank lending.) Under conditions of general financial confidence, this facility is welcomed as a business opportunity for banking institutions, as a quantitative relaxation of credit restrictions for borrowers, and as a general adrenalization of the wider economy through increased liquidity. Historically, the resulting incentive structure brought banks, borrowers, and governments into alignment, in the direction of financialization (or compressed reserve ratios). The attractions of money creation are so self-evident they obliterate the counter-factual case.[274] How could the financial alchemy of fractional reserve lending, with its seemingly magical multiplication of profits, borrowing opportunities, and commercial stimulation, conceivably have been resisted? And once it had ceased to be resisted, what could possibly have gone wrong?

§5.56 — On the opposite side of the ledger, multiplication of credit money through fractional reserves was balanced by the unplanned invention of a new type of credit risk. Local default was now potentially amplified to the level of the global bank run. The credit multiplier, when toppled into reverse, became an engine of financial catastrophe. Quantity has a quality all its own.[275] Systematic banking crisis posed an existential threat to political regimes.[276] The risk involved, therefore, tended – as a matter of sheer

---

[274] The armchair mode of estimation is, of course, wholly pedagogical, or dramatic, and insofar as it suggests harmonious concordance of contemporary financial norms with timeless human intuition, it is positively misleading. From the perspective of trans-historical anthropology, the only natural money is metallic. It was necessary for bank-money to build a new financial 'common sense' for itself. The success of this project has been so remarkable that it is has eclipsed acknowledgment of its radical historical contingency. It nevertheless has to be recalled that the adoption of this monetary regime has been late and rare (even singular). … The reconfiguration of money through institutional credit creation found its concrete historical ratchet not in the parlors of policy deliberation, but on the battlefield. In other words, it effectively financed the geopolitical occasions for its own entrenchment. To a considerable extent, British military history since the beginning of the 18th Century has been its testing ground (a claim that is smoothly extendable back to the independence struggle of the Dutch Republic from the end of the 16th Century). By providing the logistical sinews for the rise of Anglophone global power, modern credit finance created the real conditions for its teleological self-validation. It organized payment for the world order in which it would be at home. The circuit of auto-production, in all its groundlessness, is evident at every scale. We return, then, to the process of nihilism and its machinery. Occidental religious crisis and modern economic history are aspects of one thing. The erosion of transcendent foundation provides the time gradient of both.

[275] According to Wikiquote, the common attribution of this phrase to Josef Stalin is unreliable. If we still hear an echo of the materialist dialectic within it, the allusion is not altogether confining.

[276] The contribution of John Law's Mississippi Bubble to the collapse of Europe's Ancien Régime has to count as the supreme example of inverse political risk (i.e. risk to a political order from economic calamity).

magnitude – to escape narrow economic categories. Confidence sets out on its long journey into becoming an explicitly-recognized macroeconomic variable. At a certain threshold, sheer aggregation of private actions transitions into a public event. Banking crisis comes as close to capturing the fulcrum of political-economic interchange as any conceptually-isolable event can. The deep tendency of modernity to encapsulate the empirical plays out into economic institutions.

§5.57 — Political recognition that a banking crisis cannot be permitted to happen finds its institutional manifestation in a central bank.[277] A central bank is the authoritative model of a trusted financial institution. Trust conservation is its principle responsibility. In one direction, it guarantees the credibility of government paper. In the other, as 'lender of last resort'[278] and provider of deposit

[277] The lucid administrative identification of systematic financial hazard as an object coincides with the exact moment at which classical liberalism dies in principle. Such identification cannot be made without a corresponding delimitation of private commercial prudence, within boundaries too constrictive for the persistence of an autonomous economic sphere. The independent economy cannot be trusted. It requires a trust supplement, incarnated in some para-political institution. Trust is recognized as the highest economic 'commanding height' and nationalized. This is, unmistakably, a process of domestication. The state (and its parastatals) no longer solicits trust, but rather claims to produce, manage, and dispense it. This provides one thread for the argument, formalized most rigorously by Murray Rothbard, that central banking is essentially incompatible with a libertarian social order. The usurpation of trust is a centralization of contractual confidence, and a conversion into an implicitly political relation. The Statist Left, in its analysis of monetary property as politics, merely discovers the Easter egg that central banking hides. The super-abundance of the central bank's de facto power relative to its de jure authority is a predictable staple of conspiracy theorizing. The United States Federal Reserve System is an especially target-rich environment in this respect. It is an institution that might have been designed for the stimulation of occultism. The pursuit of public purposes through private institutions reliably does this. At the most basic level of analysis, the Fed is simply not well hidden. It cannot but show its work. The deliberate conversion of distributed commercial-industrial capability into concentrated national power happens comparatively recently, and in public. It is almost impossible to miss the Siren call of the imperial project, which cements the problem of trust into geopolitics. As a pseudo-transcendental being, the central bank simulates the intrinsic obscurity that is the signature of the thing-in-itself. Supposedly located beyond the ravages of crime and politics, it invokes a higher realm. Between an object of reverence, and one of paranoid anxiety, the distinction is slight. The dominating, common element is a strategic impression of abnormality. The central banker, properly understood, is a figure more at home in horror fiction than social history.

[278] The formula 'lender of last resort' was originally minted (in 1797) to define the financial-institutional role of the Bank of England. Its first appearance is found in Sir Francis Baring's Observations on the Establishment of the Bank of England, published that year. Its wide circulation, however, owes more to the later usage by The Economist editor Walter Bagehot, in his book Lombard Street (1873), which explicitly ties the therapeutic power of the general guarantor to its currency issuance authority. Some non-trivial measure of Victorian economic-moral continence can be seen in Bagehot's insistence that the exceptional relief from risk offered by the central bank should be tightly bound to explicit penalties (just as the preservation of incentives within the poor relief system required an overt punitive element). Strategic laxity requires a compensatory super-addition of discipline. This is not an equation post-Victorian society has been able to sustain. Varieties of relief disorder become,

insurance it delegates trust to subsidiary banks, in exchange for submission to regulatory oversight. The buck stops here, metaphorically applied to the desk of America's Commander-in-Chief, is more appropriately conceived as a functional definition of the central bank. While embedded, in principle, within administrative and judicial hierarchies supporting super-ordinate authorities, in practice the central bank's concentration of competence (and information) immunizes it against further transcendence. It is, in effect, a final court of appeal, or last ditch. In the sphere of economic trust, which is also that of modern economic virtual catastrophes, anything the central bank cannot stop, cannot and will not be stopped. The peculiar status of the central banker appears, to skeptical observers, near-Messianic. This is an impression that reaches far beyond trivial coincidence. In the end, which it incarnates, financial trust – 'confidence' – is the central bank's sole specialism. All of its functions converge upon this, as upon a compact telos. Implicitly, savers trust their local bank because they trust the central bank, and they trust the central bank despite their distrust of the national government. Notably, it is a structural component of modern political ecology that governments expect their national central banks to be trusted more than they are trusted themselves. They in fact come to depend upon this, as the first convincing modern substitute for divine sanction. Government deference to the central bank serves as a credogenic ritual. Through the pseudo-transcendence of the central bank, administrative politics is able to gesticulate beyond itself, to a superior source of credibility. Practical metaphysics is thereby exemplified.

§5.571 — Central banks do not (of course) monopolize the status of the trusted third party, but they provide its most concentrated and perhaps also most self-conscious example. The function of transcendence in socio-economic systems has no superior illustration. The central bank is a part of the financial process that is at the same time deemed above and outside the process. Integral to its identity and operation is the presumption that it transcends the constraints and incentives generally characterizing the financial sphere. Central bank profitability, for instance, is remarkably discreet. The public profile of the institution is incompatible with a commanding drive to make money. Something like radical altruism is tacitly insinuated, as if in pre-emptive repudiation of Public Choice cynicism. Reciprocally, resource limitations on central bank discretion are strategically de-emphasized. While not positively pretending to infinitude, or an unlimited capability for monetary intervention, some rough functional facsimile of such is not strenuously discouraged. Because the central bank is effectively a final institution, those wastes of potential financial catastrophe lying beyond its scope can only be populated by dragons, and are therefore rendered in certain respects unthinkable. The end of the world

instead, the normal condition. The asymmetric "Greenspan put" – which protects investors against losses without any reciprocal constraint upon gains – exemplifies the syndrome.

is re-articulated. There is a theatrical and ceremonial dimension to all of this, which has not gone unnoticed, or unmentioned.[279] Central bankers are – in the strictest possible sense – modern magicians.

§5.572 — Every central bank is an amphibian, or a Janus-faced being. Operational pseudo-transcendence requires this. The central bank mediates between the public and private aspects of the economy – and even defines the distinction between the two – drawing upon the institutional axiom that aggregate confidence in private commerce is a legitimate, and inevitable, target of public policy concern. Trust, in its distributed economic manifestation, is taken as the object of a mass social technology. The great macroeconomic conception occurs, pre-programming much of what then follows. The critical point is the recognition that money issuance is a policy tool, precisely insofar as it is a channel of public communications. It is no longer that money merely bears a message, in the manner of a minted coin adorned with various politically significant inscriptions. A Federal Reserve note still carries such signs, but their seriousness is entirely eroded. Money-making, as such, is now the message. Aggregate liquidity management is no sooner adopted as an administrative responsibility than it flattens upon its own public enunciations. Signal and substance are one. A teleological transition occurs here, that might easily be missed. 'Public' (i.e. state) revenue maximization, an obvious goal from at least one perspective, yet one that has been evidently instrumental in regards to the obscure practicalities of historical installation, is absorbed into a more complex structure of purposes. It becomes the opportunity for a public demonstration – for publicity. Hence the distinctive emphasis placed upon the central bank statement, an address not only about, but to the market, spectacularly totalized from above. This is already to say that irrespective of its intentions, or self-comprehension, the central bank inherits responsibilities that are strictly magical.[280] Vivid 'materialization' of the

[279] Alan Greenspan provides an especially dramatic example of central banking as public performance. No one has more clearly articulated the explicit duty of the central bank to make its decisions ineffable. As he famously remarked: "I guess I should warn you, if I turn out to be particularly clear, you've probably misunderstood what I've said." Ironically, the critical invocation of abstraction is entirely undisguised. It is not confidence in anything particular that the central bank is properly concerned with, but rather pure confidence, as manifested in monetary intensity, or liquidity. Concrete policy presentation is thus conceived as a new species of idolatry, to be jealously avoided. When John McCain later joked that in the event of Greenspan's death he would prop up his corpse in dark glasses and hope that nobody noticed, the same magic theater was being referenced. Between the appearance of financial authority and its reality lies no difference that matters. Trust is practically aligned with the paradox of a supernatural phenomenon – of the 'phenomenon' in its colloquial rather than philosophical sense. One sees only that what one sees could not possibly be enough. A 'leap of faith' is therefore modeled, from the other side. To be catapulted into credence is the desired effect. That is the entire point of the show, and everyone knows it. The audience is to be healed of its skepticism, in something like the Reformed Christianity revivalist style. Belief is the essence. Expressed within the suitable Protestant idiom, financial salvation is earned by faith alone. That Macro has come to sound like a Stephen King plot is only by shallow estimation a coincidence.

[280] The systematic taxonomy of magical effects remains an under-developed and controversial subject. No general consensus exists as to whether a full categorization is possible, still less is there any agreement as to its final

impossible – i.e. of free risk relief – is its central obligation. It is not only illusionism that is at work here, then, but medicine, or therapy, in accordance with the archaic role of the witch-doctor. The public utterances of the central bank are a mass psychological talking cure, but inverted from an exercise of attention into an incantation, and thus a spell, or placebo. We hear in these words the technical ideal of the confidence trick, in its super-legal and pseudo-metaphysical configuration. Practical efficacy is tacit. Like credit money itself, the truth of the central bank statement is created – ab nihilo – in being believed. The reality is ideally exhausted by the phenomenon. It is what it is thought to be, and no more. Confidence, in the end, has no ulterior derivation. It is miraculous.[281] Half a millennium of demystification has led to this, clearing the stage for business-suited new magicians. The performance is underway. A tranquillized collective economic sphere is to be conjured into existence. As it entered its advanced maturity, The Great Moderation named it well. The Great Moderator – Mighty Macro – is a more valuable name still, for the One at the End who Looks Both Ways to Make Peace. That's the Magician-God in the Bitcoin cross-hairs.

§5.573 — On the empirical plane, a trusted third party functions as an intermediary between a pair of agents. It is the mutual relation to a common intermediary that formally determines the agents concerned as peers. Virtual lines of evasion (route-arounds) cross the plane, linking the mediated agents in innumerable alternative ways. When plotted upon this flat expanse, the trusted third party appears as an interception – something like a successful hunt, an act of capture, or captivation. On the plane, every overseer is exposed as avoidable, if not in actuality avoided. There is always another way. Excessive impositions prove repulsive. Every moment of mediation has therefore to strike a bargain. No hint of the universal is found here. It is not upon the plane, but upon the pseudo-distinct, pseudo-orthogonal, and pseudo-metaphysical axis transecting it that the exorbitant authority of the overseer is 'for the first time' expressed. The horizon of supervision extends into the infinite. If not explicit in its

architecture. The most disciplined attempts to complete such a project, however, tend to concur on the prominence of production and vanishing as elementary magical effects. Creation (ex nihilo) and annihilation are the theo-cosmic archetypes. Stage magic dramatizes ontological modality. Monetary conjuration complies neatly with this scheme. In the era of financialization, credit expansion and contraction attest to an absolute process of money production, 'backed' by nothing beyond itself. At the limit, money demonstrates radical insubordination relative to the question of being. With all material constraint on minting lifted, monetary production submits only to magical will. In this context, Bitcoin looks like a spell cast during a magical war. Its restriction upon money creation is characterized by unprecedented severity, from one regard. From another, however, the entire crypto-currency is an ex nihilo creation, bringing a virtual BTC 21,000,000 into existence spontaneously, out of nothing. Money creation switches phase. It is no longer amplification, but sheer innovation. Reciprocally, an updated model for monetary annihilation can be expected, no longer based on credit contraction, but rather on crypto-currency extinction events. Proliferation and culling of new currencies begins to increasingly regulate the money supply. Cryptic sorcery contests financial magic.

[281] It is the sacred calling of skepticism to doubt the existence of things whose reality inheres in nothing beyond their being believed – but not to the point of dogmatism.

claims to omniscience, omnipotence, and omnibenevolence, it makes no effort to dispel such theological encrustations. An implicit invocation of God-like powers follows from the conspicuous assumption of God-like responsibilities. In wherever the buck stops we trust. The aura of infinitude is essential. No limit can be drawn. Whatever lay beyond the outer boundary of central banking power would be the lair of crisis, by definition. A formal delimitation of the supreme third-party powers is indistinguishable from a program for financial catastrophe.[282] Agreeing not to go there closely coincides with the new social contract, drafted in the 1930s. Critique of authority henceforth meant Great Depression. To the titles of Macro can then be added: The Unscrutinized Scrutinizer. That which sees all should not be excessively challenged by inspection.[283] This is how asymmetry has been put to public work. Apparently exempted from immanence, the overseer is fed by the impression of exceptional rules, and sublime incentives. It seems to hover above the fray, as if released from mere empirical difference into a superior milieu. Amphibious by essence, it is at once an efficient, individualized, economic agent among others and simultaneously nothing at all of the kind. The effect works best when no one looks too closely.

§5.58 — Central banking did not begin with the Bank of England, in exactly the same way that terrestrial capitalism did not originate among the Anglophone Powers. This is to say that a comparable 'usurpation of destiny' – in the full ambivalence of the term – is evident in both cases. Fate was settled on an English path, which took work.[284] An obscure opportunity for supra-national influence was

[282] "Only a god could save us," Heidegger remarked in a 1966 Der Spiegel interview. The mature world credit-financial order was not the primary context for these words, but it might aptly have been. An overseer who is definitely less than a god is nothing. Where deity is slow to unambiguously manifest, ceremonial magic is required to make up the difference.

[283] Is not the illusion of vision among our most consistent themes here? The Federal Reserve Note includes the picture of an eye. It is not meant even to be noticed. To feel oneself perceived suffices for childish comfort. Claims to see rarely tolerate close examination. Intense scrutiny ruins the effect. This is now what we are seeing.

[284] Within six years of the 1688 'Glorious Revolution' and the installation of the Orange monarchy, the Bank of England was born. It is difficult, therefore, to miss seeing a transnational socio-historical project at its root. Many nations undoubtedly find a way to frame their fate exceptionally, within the terms of a mission exceeding common geopolitical interest. A country is thus conceived as a vehicle for something other than its people. The Glorious Revolution illuminates the English version of this. Protestantism and – more profoundly – capitalism is the cargo. Neal Stephenson's 'Baroque Cycle' of historical novels captures the process in its cultural essentials. National independence, holy war, and unprecedented financial technology composed an original compact system. Catholic 'conspiracy theory' in this regard is not unwarranted. The hostile perspective of an E. Michael Jones brings out the contours of this new thing more sharply than its liberal defenders can. It was built so that schismatic theology might prevail in global conflict. With all due diligence to the hazards of unfettered teleological apprehension, it remains near-irresistible to ask: What was the Bank of England designed to finance? Nothing less than a planetary revolution could count as an adequate answer. The Dutch Revolt or Eighty Years' War (1568-1648) had set the template. Advanced financial infrastructure offered near-miraculous strategic geopolitical advantage. The defeat of the Spanish Empire in the Dutch independence struggle meant that the culture of

captured, and became self-consolidating, through convergence. Which is to say: the occasion for financial elaboration found its strongest expression on the supra-national line. It was, from the beginning, world-historical.[285] In the final analysis, it has happened to peoples more than from them. Teleological instrumentalization of the English-speaking peoples, as agents of global process, has been no less basic than their adoption of new financial technologies. The two developments have been one. Central banking has been nationally functional to the exact extent it has been internationally competitive, and thus globally compelling. It won wars that mattered, first for the Dutch, then for the English. By the time the United States inherited managerial responsibility for the world order, its principles of financial sovereignty had been firmly set in place. The task of managing the national debt was, as a matter of concrete practicality, a military logistics function. It assured war-fighting capability at the highest level of strategic abstraction. Whatever was needed was made affordable. The consequences were consistently dramatic. Because the states that quickly took the lead in central banking were – not at all by coincidence – the successful vehicles of a supra-national (or global-revolutionary) undertaking, nothing like a simple nationalization of money was ever actually happening. Rather, the production of international reserve currency was becoming reflexive, and institutionally self-aware. This does not make monetary nationalism a mere illusion. The organizational level of the nation state did in fact become increasingly dominant, and all the more so when international adventure

---

modernistic schism, or autonomizing capital, would not be stopped. No future foe would present comparable challenges, whether estimated in terms of the apparent balance of forces, or even the clarity of ideological decision. Globalization in the 'neo-liberal' sense was henceforth implicit, dominating the historical horizon of the world. All of its subsequent contestants would be compelled to articulate their resistance within a framework fundamentally shaped by the liberation of Capital, and benchmarked to it.

[285] There is no doubt a Globalist Idea and most probably several. The Oecumenon tilts towards one. (One is never less than simply compelling.) It would be precipitous, nevertheless, to assume that the supra-national points unambiguously towards global unity. Delocalization and globalism are synonymous only under strained dialectical assumptions. It takes more than an entire planet to complete the logical sense of a globe. Comprehensive globality has no possible empirical instantiation. Proselytizing religion is its natural territory, and it evokes concreteness only to mock it. From the perspective of oecumenical globalism, the empirical process necessarily underperforms at oversight. It is, critically, excessive in its singularity. Ethnic peculiarity, in particular, inflects it. There is no side-road back to the universal, even through a conception of ethnic peculiarity in general. Capital escapes exactly once. It therefore shrugs-off generic characterization. Concretely, within modernity, 'supra-national' has meant predominantly Anglophone. In addition, the requirement for expertise at delocalization almost sufficed in itself to ensure significant Jewish involvement, which the Protestant revolution notably facilitated. In can therefore be insisted, on grounds exceeding firm analogy, that globalization is not a project, in precisely the same sense that there is not an International Jewish Conspiracy. Which is to say that there is in both of these cases really something – and even the same thing – manifested as a structure of fate, though without commanding deliberation. The conspiratorial interpretation is encouraged (and simultaneously misled) by the fact there are not here simply two different things. Ayn Rand's widely-derided identity assertion ("A = A") finds productive application on this point. Capital – as historical fatality – is what it is and nothing more.

was at stake. It did not, however, control its own context. The supra-national process preceded, exceeded, and catalyzed all national developments, because the battlefield was the arena of selection. The history of central-banking is bound far more tightly to the production of world-money than happenstance could account for. The global revolutionary mission was primordial (i.e. essential, or intrinsic). In contra-distinction to the financial myth, sound domestic money management did not simply come first.

§5.581 — The Bank of England was incorporated by the 1694 Bank of England Act. However much centralized monopolization of bank note issuance now looks like the basic destiny of the institution, it was only very gradually established, over the course of more than two centuries of subsequent legislation.[286] It was not, therefore, a guiding project (in anything other than an obscure teleological sense). Monetary nationalism was only a slowly emerging outcome. It was fiscal nationalism that provided the primary imperative. Twin agendas were originarily complicit, directed at once to domestic financial stabilization and to state revenue-raising with a definite outward, geopolitical orientation. The incorporation of the Bank, then, marked a further step in the integration of modern banking with sovereign political power.

---

[286] The first Bank of England notes were issued in 1694, the year of the bank's founding. Initially, they functioned as bank checks, written for arbitrary sums. Their denominations were not standardized until 1745. Large notes predominated. The smallest note issued by the Bank was £20 until 1759, worth £3,300 in 2017. Innovation tracked the cycles of the war economy. The first £10 note was issued during the Seven Years' War, the first £5 note during the war with revolutionary France (in 1793), followed quickly by temporary £2 and £1 notes before the end of that same conflict, and the century. These early notes were units of government debt, but not circulating currency. It was not until 1855 that they became payable to the bearer, and thus freely exchangeable. In keeping with their new function as currency, the notes became entirely machine-printed in the same year. Previously, of course, standardized national currency production was the exclusive responsibility of the Royal Mint, as it had been since AD 886. Monetary transition into the fiat regime has been tracked by the rise of the Bank of England, and reciprocal marginalization of the Royal Mint (which continues to manufacture UK coinage to the present day, although now out of intrinsically near-worthless base metals). Issuance monopoly came slowly. Even the smallest banks were permitted to issue their own bank notes prior to the Bank of England Acts of 1708 and 1709. Currency issuance was actually liberalized by the 1826 Country Bankers Act, extending the right to print money to joint stock banks (meeting certain criteria of size, and distance from London). It was only with the 1844 Bank Charter Act that monotonic progression towards Bank of England currency monopolization was set unambiguously in motion, with removal of note-issuing rights from England's last private note issuer (Fox, Fowler and Company of Somerset) following its acquisition by Lloyds Bank. The process was not fully completed until 1921. The comparatively rapid demotion of the UK from the geopolitical responsibilities of recent centuries took place over a small number of subsequent decades. Partial convergence with a broader European trend to currency integration was an indicator. The pound was only decimalized in 1971, following the entry of the UK into the European Common Market (predecessor to the European Union).

§5.582 — The much later US central banking Federal Reserve System is far more arcane than the Bank of England. It dates back only to the final days of 1913, as a creature of the Federal Reserve Act, through which Congress announced an American public (i.e. national) monetary policy. The institutional origin of the Federal Reserve is explicitly inseparable from a post-liberal ideology of money, which conceives it as an administrative tool, to be placed in the service of national economic objectives (the macroeconomic suite of full-employment, stable prices, and moderate interest rates).[287] The British experience had been educational, in this regard. Money had been re-minted as an imperial project, with twin global and domestic faces. Where the Pound Sterling had found itself elevated by fortune to the status of imperial scrip, the US Dollar now ventured onto the same path of geopolitical fatality with greater self-consciousness. The relation to war economy was effectively deepened. By the early 20th century it was obvious to all observers that the primary Anglophone world power could have no (merely) national interests that were not immediately matters of global geostrategic and ideological competition. The US Dollar could only be an architectural pillar of world order. To trust it was direct psychological investment in a planetary destiny.[288]

---

[287] The US central banking Federal Reserve System came into being on December 23, 1913, with the enactment of the Federal Reserve Act. The brief of the new institution, quite explicitly, was to subject financial market psychology to centralized governance. Specifically, it was designed to suppress panic. The most immediate reference was the 1907 Banker's Panic or 'Knickerbocker Crisis' (named after the Knickerbocker Trust Company whose collapse triggered the nationwide financial catastrophe). In keeping with the modern formula, bank-runs had been the primary driver of cascading insolvency. Under American institutional conditions, there was no circuit-breaker in the process. This was the conclusion of an investigative commission into the panic, established and chaired by Senator Nelson W. Aldrich in 1908, which identified the country's lack of a central bank as the root cause of the crisis. The Aldrich Commission proposals led directly to the creation of the Federal Reserve System. The new institutional structure, named with misleading simplicity as the Federal Reserve (or just 'the Fed'), was characterized by Byzantine complexity. Its Board of Governors has seven members, appointed by the US President (subject to Senate confirmation) for 14-year terms. In order to maximize administrative continuity, and manifest independence, one member is appointed every two years (in a 14-year cycle). In addition, there are twelve regional federal reserve banks (FRBs). The entire Board is supplemented by five presidents from the regional FRBs to compose the (twelve-member) Federal Open Market Committee (FOMC). In recognition of its status as the nation's financial capital, the New York City FRB is privileged with a permanent position on the FOMC. It is the FOMC that wields primary executive power within the system, practically directing national monetary policy. Finally, the (private) banking industry is provided with formal consultative representation within the system, through the twelve-member Federal Advisory Council. In respect solely to the occult social status of the Federal Reserve, the most appropriate comparison might be to The City of London (as an institution). William Gibson makes this private crypto-governance (whose medium is the open secret) a theme of his time-travel novel, The Peripheral.

[288] In God we Trust, the official motto of the United States of America since 1956, began to appear on the country's paper currency in the following year. It had already been struck onto coins for almost a century (beginning in the Civil War year of 1864). Over the course of three centuries, the implicit commitment underlying

§5.583 — Under conditions epitomized within the era of matured central banking, but by no means restricted to it, monetary value reduces ultimately to a political substrate, where confidence is maintained by evidence of effective power. This registers a critical inversion. The capacity to protect property begins to 'appear' – i.e. to trade – as its essence. Recognition of the 'protection racket' as a mode of criminal enterprise closely coincides with this development in time. Investors – including even mere holders of currency – have been re-sensitized to regime risk, which sub-divides into two broad (but intricately inter-articulated) categories. Firstly, the 20th Century has dramatically featured sheer expropriation, of the nationalist-communist type. In response, assets of any kind now feature some degree of Marxist discount. They are priced with a measure of definite regard to their vulnerability to government seizure, or 'revolutionary redistribution', which automatically increases yields in the most hazardous cases. The antithesis is practically assimilated. Secondly, and more subtly, political authority has been increasingly formalized as an asset class. No longer merely devoted to the protection of property, whether to a greater or lesser extent, it has itself become an object of comparatively direct financial investment. Government bonds offer a share in imperium. They securitize regime resilience and demographic purchase, or geopolitical capability.[289] Under conditions of global stress, most conspicuously, the lender of last resort transitions into a debtor of last resort, and thus a savings facility, socializing deferred private consumption through the medium of public financial obligations. The Federal Reserve Note is nothing less than a wager upon the future of America, its central government, and – most specifically – its taxation power. By extension, the exceptional global acceptance of the US dollar is an investment in American world order. All these relations are analytically reversible. Geopolitical crisis implies currency crisis, or – still further – potentially follows from one. The coin has two sides, and can be easily flipped. 'Derealization' into pure credit only accentuates money's ambivalence. As it is incrementally demetallized, money takes the form of a promise, whose credibility is founded upon the public image of state power, as fully-expressed within both domestic and international contexts. Under such circumstances – especially when a global hegemon is in the spotlight

---

the monetary credibility of the world's principal English-speaking power had escalated from (the 17th century) Protestantism will survive to (the 20th century) Anglophone global capitalism will prevail. The difference is primarily cosmetic. Those oblivious to the core identity of Protestantism and Capitalism understand neither, or the fact each is the occult aspect of the other. Schism and automation are the guiding threads. The Great Seal of the United States, with its twin mottos Annuit Cœptis ('our undertaking is favored') and Novus ordo seclorum ('New order of the ages'), has decorated Federal Reserve notes since 1935. The intensity of Federal Reserve conspiracy-theorizing has not, of course, been harmed by this.

[289] As Niall Ferguson remarks in The Ascent of Money (p.102), while describing the economic consequences of the First World War: "Those who had bought war bonds had invested in a promise of victory …" Insolvency then follows from an erroneous interpretation of destiny. At work here is an economic domestication of geopolitical risk. If any single index captures bourgeois nationalism, it is this. Private savings are explicitly invested in a national-collective undertaking. No less notable is the dynamic of self-reinforcement, accentuated by survival bias. One thus sees in the bond market political economy being synthesized in real time.

– the stakes of a 'monetary revolution' are not easily over-estimated. Nor are its positive implications readily anticipated. The nature of money has long ceased to be separable from the order of the world.[290]

§5.59 — As financial modernity advances, 'printing' becomes an increasingly unreliable metaphor for money creation, even as paper continues to support its metaphors. The engine of currency production is no longer any kind of minting or printing, but (fractional-reserve) credit. At the limit, the formula of the Macro epoch is an equation of money and debt. Its foundations are as old as Modernity, but no older. Mere centuries sufficed for it to fabricate the illusion of something more archaic, or even eternal.

§5.591 — Political economy is an apparent identity, but a real synthesis. It requires a coupling mechanism. Concretely, the crucial communication medium has been the bond market.[291] Given a fixed coupon, the effective interest rate will vary as the reciprocal of the bond price. The yield on government paper thus articulates a 'market verdict' on the political regime. It expresses something far more valuable than ideological affection, namely pragmatic confidence. The question addressed is only: Will this work? While stated confidence in government is communicated through a variety of professional channels, media, and electoral processes, revealed confidence is expressed through secondary markets in public debt. The bond market has provided such automatic commentary since the beginning of the modern period (already operating in the city states of Renaissance Italy), and can even – again concretely – be identified as an essential or defining component of modern political-economic governance. Capitalism might – quite sensibly – be taken to mean precisely this, at least up to the point currently reached. Political regimes make themselves an object of economic investment, inviting private wealth-holders to 'go long' government. Because this mechanism enables – to some effective degree – private markets in public policy, it provides the Macro regime with its most important feedback control. We meet Janus again (as with every social regime). Political-economy is only Janus' modern name. The ambivalence is the engine. A hinged singularity produces effects of pseudo-universality on its public face, and intelligible incentives on its private face. Continuous temptation to resolution, in one or other direction, adds camouflage as a supplement. There's a simple story you want to tell, which is how it hides.

---

[290] At the world-scale of the economic hazard transitions into transcendental risk, where the stake is nothing less than the system in its entirety. The whole cannot be hedged. Wild bets on, or against, the future of capitalism stretch the competence of markets to their outer limits.

[291] By productive irony, the primary meaning of the bond market is a secondary market in government paper. Efficient feedback is the result of a substantial step removal from participation. There is no direct engagement with the government here at all. Rather, there is something like detached commentary, but with every intellectual commitment put to the test, through bets. Neither citizen involvement, nor journalistic opinion, then, but an index of political-economic judgment supported by real incentives, and characterized by unprecedented objectivity. It is retreat from the public sphere – in both its practical and epistemological aspects – that allows for its neutral evaluation.

§5.592 — Money has fully absorbed the ambivalence of political-economy. This has made it cryptic, quite beside it becoming cryptographic. It invites misapprehension. Of course, it is no secret that, historically, the promissory value of paper money has been very specifically tied to the prospect of redemption in precious metal. It is in fact almost, though not quite, the precise opposite of a secret – an anti-secret. With the consolidation of Macro, this has matured into a type of tolerated hypocrisy, and something like an inside joke. A concession to tradition is made where it appears most harmless. Much more is happening here, though, than a joke. The persistence of this image of value advances metallic durability into an abstracted dimension. Whenever money is momentarily jolted from its constitutive – cash-like – amnesia, it grates upon metal memory. Sheer semiotic inertia would suffice to ensure this, in the absence of any additional considerations. The Mises Regression Theorem acknowledges the same track-marks. Despite the appearance of anachronism, at no stage has this concrete definition of monetary obligation been formally updated. It has merely been repudiated. The commitment is restated without being maintained. This preserves it as a dramatic violation. To describe it as ritualistic sovereign transgression is not an excessive stretch. The repudiation of metallic obligation has been politically spectacular. Overt contempt for a nominally enduring formal constraint was itself sold as a viable – and indeed overwhelmingly dominant – socio-political position. The mass psychology of the New Deal remains entirely unintelligible until this is understood. The abuse was the attraction. In this way, as in so many others, the New Deal was classically fascist. When unleashed executive power is the selling-point, there is no inclination to conceal the broken leash. It takes the trampling of old constraints to legitimate a Caesar, and it takes a Caesar to master popularity. Only hopeless naivety would recognize FDR as anything else.

§5.593 — Ever since the gold standard was ended, the principal support for monetary value has been the state guarantee of its acceptance for the extinction of tax obligations.[292] By denominating their exactions in the national currency, and thus authoritatively defining their medium of internal revenue, governments are able to support a very substantial demand-floor for their own paper (whether currency notes or bonds). Within this arrangement, socialist and nationalist themes are merged, without significant remainder on either side. Government market-making of this kind – in which the state operates as a customer – fulfills an important mercantilist function. In most modern societies it has a wide domain of application, extending typically across business sectors more-or-less plausibly classed as 'strategic'. Nowhere beyond the monetary sphere, however, is such a mercantilist program comparably cloaked by the purity of administrative fiat. The barrier posed to the adoption and spread

[292] Paul Krugman unexceptionably remarks: "Money is a pretty amazing thing. Why does a piece of green paper with a dead president on it have value? Ultimately, it's because other people believe it has value, and [it] circulates. However, there is an anchor for dollar bills which is not gold. It is the fact that you can use it to pay taxes."
See: Thomas Piketty, Paul Krugman and Joseph Stiglitz: The Genius of Economics
https://www.youtube.com/watch?v=In7qmVNz10c#t=1h06m13s

of alternative currencies by the normalization of state-centric monetary nationalism vanishes beyond the horizon of public perception. It is only on the global periphery – among economies that are to some considerable extent 'dollarized' – that the nation state's monetary power remains naturally conspicuous (and thus susceptible to refusal).

§5.594 — The spontaneous cosmopolitanism of the precious metal coin exposes – through contrast – the historical peculiarity of 'globalization' in the age of monetary nationalism. Metal maintains an exteriority in relation to the minting regime. Its value indexes a substance outside political dependency.[293] Government paper, in contra-distinction, requires additional institutional support. The decentralized verification process of the assay is not available, or relevant. What matters for verification now is only the authenticity of the statement, whose negative is forgery, or counterfeiting. The currency unit is irreducibly invested in its regime of issuance. Thus, forex operations become an institutional subspecies of international relations. Acceptance of a currency now implies substantive – rather than merely formal – political recognition. There can only be foreign exchange once the right to make promises has been granted to all relevant regimes.

§5.6 — Once extracted from a domestic competitive environment, through establishment of a state monopoly of currency issuance, money supply is exempted from commercial spontaneity and becomes a macroeconomic problem. This is to say that it acquires the status of an overseen aggregate. Money is no longer conceived primarily as a kind, or as a distribution, but as a whole. It is envisaged in entirety.

§5.61 — It might be asked whether the term 'macroeconomics' has anything reasonably described as a common usage. The word is intrinsically extraordinary. It implies a very specific structure of professionalization, and credentialized expertise. In its maximally-reified sense – as it is employed here – it also has a designation that might escape familiarity, and certainly seeks to. Macroeconomics is not merely an intellectual domain, or its corresponding social object, but a regime.[294] Positive institutions

[293] The world's first international currency of modern times, the Spanish Real de a Ocho or 'Piece of Eight' (Peso de Ocho), was a silver coin that monetized the precious metal acquisitions of the New World. Its value was invulnerable to hypothetical collapse – or even comprehensive annihilation – of the Spanish empire. The regime risk borne by those holding it was zero. Reciprocally, it involves minimal regime complicity. The Spanish empire was not being in any serious way automatically endorsed by those holding or trading in its currency. Hence classical mercantilism sought to deny foreign access to the national currency, with 'losses' of treasure analogized to bleeding. Since geopolitical legitimacy cannot be propagated through metal, no regime incentives exist to promote its diffusion.

[294] Is Macro a regime, or does it decompose (diachronically) into regimes? The question might be inelegantly re-phrased: Would this vocabulary not better be reserved for a compendium of macroeconomic regimes (plural), in the sense that, for instance, Mark Blyth uses the term (to distinguish, in particular, social democratic and neoliberal eras)? The significance of the transition at the center of Blyth's analysis is beyond all serious controversy. Yet, upon examination, the problem tends to self-liquidation. Social democracy underwent

are essential to it. These cross, consistently, between the realms of academic research and social administration. The theoretical procedures under consideration here are essentially managerial, shaped originally by policy orientation. The model macroeconomic thought-experiment takes the form: What if the government did X? Thesis and recommendation are one. Macro never speaks, then, without a side-address – at least – to the state. Power is endogenous to it. The ambiguity between Macro the thing and macroeconomics as a research domain naturally – and strategically – elicits confusion. Macro is a singular catastrophe in the technical sense, which is to say a systemic phase transition, but also – from certain inherently fragmentary and now systematically marginalized perspectives – an actual socio-historical disaster. The clue to Macro, so telling as to pass almost for a synonym, is oversight. It is lodged in that part of the social organism tasked with supervision of the whole.

§5.611 — Between the whole and its parts lies something more than a difference in scale. In no case does one simply scale-up to totality. The whole appears only to oversight (or is made to seem so). It is thus tempting to conceive macroeconomics as a structure of visibility.[295] Its essence is defined by what is called to appear before it. Any tribunal is like this. The economy is to be brought before Macro for inspection, judgment, and correction. Macro, then, is a massive, complex, pseudo-transcendent operation in the name of the whole, conducted upon the axis of trust, or confidence. It is the metaphysics proper to the economic realm. In the alien language of German idealist philosophy it might be characterized as central banking for-itself. In this respect, among others, it could not be anything other than the mainstream magical tradition.

§5.62 — On the singular path actually taken by the world, money is recomposed as a Macro aggregate, the money supply. Under retrospective consideration, some such thing has long existed. In the same way, volcanoes erupted with a bang before anything with ears could hear them. But it is only in this way that Macro aggregates pre-existed the managerial structures which formulate them. The model of money as debt has limits, and thus provokes critique. Neither precious metals nor crypto-currencies can be assimilated to it. Positive monetary assets (collectibles) are its unthinkable outside.

---

neoliberal transformation at the point when its stagflationary crisis became politically unsustainable. Unelected central bankers could do what democratic politicians could not (save the system, through 'sado-monetarism' – to use UK Labor Party Chancellor of the Exchequer Dennis Healey's apt expression). The break, nevertheless, occurred within Macro. Regime continuity was its presupposition. Between social democracy and neoliberalism there is nominal independence, but dynamic complicity. The latter corrects the former, and makes no sense outside this context. It was a reaction, of near-mechanical predictability. Macro encompasses the oscillation.

[295] James C. Scott's Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed undertakes a celebrated critique of 'high modernism' conceived as a system of visibility. Its mode of analysis thus bears comparison with Foucault, in applying philosophical criticism of the construction of objects to the social field. Such analysis, predictably, has distinctively anarchistic slant.

§5.63 — According to the quantity theory of money, money supply determines the general price level. The economic consensus on this point is so broad it approaches recognition of a tautology.[296] After all, it would be strange indeed if money – the model object for economic estimation – were to be exempt from elementary principles of supply and demand. Although meeting a reception in popular culture appropriate to a tendentious claim, Milton Friedman's succinct maxim that "Inflation is always and everywhere a monetary phenomenon" is in actuality almost entirely uncontroversial. The fundamental idea is one that even the Antichrist of today's hard-money advocates, John Maynard Keynes,[297] subscribed to – without serious hesitation. Any instance of economic value is a registration of scarcity, and the value of money is only a special case of this general rule. It is, of course, in recognition of this utterly pedestrian claim that scarcity is included in any list of the essential properties required by a monetary medium. In the extreme case, glut destroys economic value. It is therefore understandable that the tendency among economists has been to negotiate the terms of this formula's application, rather than to challenge it at a fundamental level. Submerged – very slightly – beneath the

---

[296] The 'quantity theory of money' (i.e. of inflation) can be traced back to Nicolaus Copernicus. Subsequent proponents have included Jean Bodin, David Hume, and John Stuart Mill, among very many others. Its insistence should not be surprising. The principle of scarcity – that for any commodity abundance is inversely related to price – is a candidate for the most basic of all economic intuitions. It is unlikely that any market agent has ever seriously doubted it. Milton Friedman writes in The Counter-Revolution in Monetary Theory (1970): "Inflation is always and everywhere a monetary phenomenon in the sense that it is and can be produced only by a more rapid increase in the quantity of money than in output. … A steady rate of monetary growth at a moderate level can provide a framework under which a country can have little inflation and much growth. It will not produce perfect stability; it will not produce heaven on earth; but it can make an important contribution to a stable economic society."

[297] While Keynes' reputation as the arch-inflationist among serious economic authorities is amply justified by his influence, it is less easy to square – consistently – with the letter of his text. His early writings are especially notable in this regard. Perhaps no one has ever understood the ruinous effects of inflation better. As he remarks: "Lenin is said to have declared that the best way to destroy the capitalist system was to debauch the currency. By a continuing process of inflation, governments can confiscate, secretly and unobserved, an important part of the wealth of their citizens. By this method they not only confiscate, but they confiscate arbitrarily; and, while the process impoverishes many, it actually enriches some. The sight of this arbitrary rearrangement of riches strikes not only at security, but at confidence in the equity of the existing distribution of wealth. Those to whom the system brings windfalls, beyond their deserts and even beyond their expectations or desires, become 'profiteers', who are the object of the hatred of the bourgeoisie, whom the inflationism has impoverished, not less than of the proletariat. As the inflation proceeds and the real value of the currency fluctuates wildly from month to month, all permanent relations between debtors and creditors, which form the ultimate foundation of capitalism, become so utterly disordered as to be almost meaningless; and the process of wealth-getting degenerates into a gamble and a lottery. […] Lenin was certainly right. There is no subtler, no surer means of overturning the existing basis of society than to debauch the currency. The process engages all the hidden forces of economic law on the side of destruction, and does it in a manner which not one man in a million is able to diagnose." – The Economic Consequences of the Peace (1919), Chapter VI, pp. 235-236.

macroeconomic argument lies the real topic, which is institutional discretion in respect to money-supply management, and therefore the politics of trust. To what extent should controlled monetary debasement be available as an option to the regime?

§5.64 — The central Keynesian argument, as formulated in his The General Theory of Employment, Interest and Money (1936), has surely to be included among the most influential in history. Its unique virtue, from the perspective of the modern nation state, was to provide a rationalization for currency debasement. No previous political power had ever been blessed with such a thing. A Roman Emperor adulterating the coinage harbored no illusion about the essential corruption of the undertaking. It was nakedly a swindle, whose advantages overrode reservation. Now, however, there was for the first time an articulate justification for what was essentially the same procedure. Macro grounds its legitimacy in the proposition that programmatic monetary devaluation can, under certain circumstances, have positive aggregate economic effects, by contributing to the mobilization of unemployed resources stranded in social 'liquidity traps'. This trade-off between inflation and unemployment – formalized in the Phillips Curve – has insinuated itself deeply into macroeconomic intuition, surviving even the complete collapse of its supportive empirical regularities during the 'stagflationary' 1970s.[298] It relates

[298] If the highly-contested term 'neoliberalism' is determined with primary attention to its historical limits, it coincides with a naïve confidence in the mortality of Keynesianism. The empirical commitment upon which it assumed Keynesianism would perish is easily sketched. According to the Keynesian Macro consensus, as it prevailed up until the late 1970s, the most fundamental relationship between inflation and unemployment was conceived as negative, or compensatory. It thus supported trade-offs. In the post-war Western order, an entire structure of socio-political negotiation had been erected upon this foundation. Dynamic tension between the quality of money and the quantity of employment opportunity became an arena – and even a proxy – for class struggle. Money was publicly degraded in the cause of social peace. The breakdown of this theoretical relationship was signaled by a stagflationary trend. Stagflation is an important word in the history of recent political-economic regimes, because it announces a cybernetic inversion. Under stagflationary conditions, unemployment and inflation advance together, without prospect of cross-substitution. They exhibit positive, rather than negative, cybernetic linkage. Between this acknowledgement and neoliberalism in its compact historical sense, there is no difference. Monetarism and Rational Expectations were the critical counter-thrusts to the prevailing Keynesian consensus. Monetarism challenged the Keynesian contention that the responsibilities of financial authorities and central banks ever extended to anything beyond conservative monetary management, oriented to price stability alone. The rational expectations analysis of thinkers such as Edmund Phelps and Robert Lucas argued that inflationary policy orientation would eventually be fully discounted, as populations factored it into their economic calculations. It worked then only in the short-term, as a confidence trick does until recognized. This period of efficacious money magic does not last long. As confidence tricks go, inflation is remarkable for its crudity. Macro, then, could not help but train its own marks to neutralize it. It was the epistemological differential between policy agents and targets that did all the work. Once the recipients of central bank scrip understood what was being done to them, it was all over. An epoch was closed. Yet the peculiar resilience of Macro to empirical contradiction is no less an intrinsic characteristic. Prolonged failure to grasp this has had far-reaching socio-political consequences. The 'neoliberal' epoch – to use the term now in a more relaxed acceptation as favored on the Left

the inflation rate to an ideal socio-political equilibrium point, and therefore defines a managerial responsibility. Money is now indexed to a thermostat. It can be too hot ('loose') or cold ('tight'). The regulatory imperative thus codified transcends any specific empirical hypothesis. The hypothesis is adjustable, and even radically replaceable. The new power, once installed, is far more resistant to retraction. Once the case for a campaign against 'cash preference' has been entrenched at the level of mass psychology, its theoretical foundations become dispensable. The communist and fascist anti-bourgeois tide of the 1930s found its principal Anglo-American expression in Keynesian macroeconomics. Here, too, 'hoarding' was denounced as a crime against the collective.[299] Implicit socialization of all economic resources was made rigorously axiomatic. There is nothing so fragile as a mere theory, here, then. Rather, there is the maturation of a socio-political program. The theory flexibly rationalizes a regime.

§5.641 — At the greatest scale of historical analysis, Macro is characterized by the way it places itself beyond the bourgeois definition of civilization. Among modernity's ascendant prudential classes, high time-preference (or low impulse-control) served as distinctive markers of barbarism. Civilization thus acquired a measure, corresponding to a time-horizon. Industrial civilization was based upon

---

– has proven strangely inept at carrying through a cultural revolution against economic orthodoxy. Its brief 'monetarist' heyday succeeded only in reinforcing the dependency of market-positive and disinflationary social outcomes on the democratic-political cycle, by consolidating their formulation as policy options. The effects of this have been predictably perverse. Those firmly market-based ('Austrian') perspectives that had opposed the rising macroeconomic regime from the point of its emergence remained entirely marginalized, excepting only a few impressionistic, decontextualized fragments, filtered through Hayek. It is tempting to conclude that the institutional requirements of academic and administrative economic authority dictated a state-managerialist doctrine in respect to money, immune to all empirical or theoretical contravention. There is here a matter of comparatively simple political right – that of oversight – masked as a complex scientific proposition. Once monetary value is based on the potential to extinguish tax liabilities, it is implicitly defined as an obligation to the state. Absolute subordination of civil society is then conceptually fundamental. It is not 'Keynesian theory', narrowly conceived, that stands in principled opposition to the autonomous determination of property and its corresponding monetary order, therefore, but rather the Macro regime as such. Radical naivety in this regard was constitutive of the late-20th Century 'Neoliberal' moment, and finally fatal to it. Macro is essentially illiberal. It cannot in any serious way be reformed. The only way past Macro is around it.

[299] The systematic macroeconomic conflation of the prudential and the anti-social is an innovation of great consequence. It prepares for the partial displacement of the Principle Political Dimension into the 'culture wars' of the late 20th century. Mere continence had now been reconfigured as an anti-social disorder. More specifically, extended private time-horizons had been made an explicit target of political denunciation. Marshmallow-test winners were the new Kulaks. Their capacity to defer gratification had been theoretically-reconstructed as social aggression, expressed concretely as a denial of unemployment opportunities to the people. Macro's cultural rebellion against impulse-control had begun. A campaign against saving (i.e. private capital accumulation) could now be conducted in the name of sexual liberation. Keynes' Bloomsbury sexuality is a crucial reference in this respect. See, in particular, Hoppe: https://mises.org/library/my-battle-thought-police

psychological tolerance for efficient indirect methods. Roundabout production had secured its ethic. Macro breaks with all of this. Imprudence is now re-valorized on Keynesian grounds as pro-social stimulation. To spend is glorious. Anti-bourgeois cultural politics and administrative economic doctrine become one.

§5.65 — When conceived theoretically – or targeted administratively – as a macroeconomic aggregate, the 'quantity of money' turns out to be an extraordinarily elusive object. Two sources of complexity are especially notable. Firstly, the effective quantity of money is a twin-factor product, comparable to physical momentum, of monetary mass multiplied by velocity (the macroeconomic 'multiplier'). Secondly, the nature of money is inherently multiple, and intensive. This is formally recognized by the systematically differentiated – and nested – monetary definitions (M0, M1, M2, M3 … Mn …MΩ) employed by economists and financial professional.[300] Any asset of non-zero liquidity is money to some degree of intensity. (Monetary intensity is approximated by the reciprocal of the index.) Between the speeds and types of money there is only illusory orthogonality, or theoretical decomposition of the diagonal.

§5.651 — The most consequential area of controversy within the macroeconomic era – with intellectual roots that can be pursued back to the 16th century – concerns the relation of the velocity of money to its quantity. According to Irving Fisher's formula MV = PQ, when the quantity of money and goods ('M' and 'Q') is held constant, the price level ('P') becomes a function of monetary velocity ('V'). Potentially, and as a matter of historical fact, an entire technoscience of monetary management follows. Any authority that is attributed with responsibility for the money supply is compelled to concern itself with liquidity. Tightening-loosening defines the control axis.

§5.652 — Given the extreme complications of technical monetary analysis, it is not unrealistic to describe macroeconomics as the monetary neo-baroque. Its elaborations are implicitly unlimited. To present its convolutions as ultimately manageable requires a more-or-less cynical public relations exercise. It cannot be admitted – for reasons of trust-preservation – that the final overseers of the

[300] Precise definitions of the monetary phases have not been internationally standardized. The principle, however, is uncontroversial. Money is defined as a series of nested categories, proceeding from the narrowest to the broadest types (with the latter enveloping the former). Monetary 'narrowness' closely tracks liquidity. The extreme of narrow money, M0, is cash. Broader phases of money include bank credits, of incrementally rising maturity, and other comparatively viscous financial assets. Typically (but with some national variance), M0 is strict cash, M1 encompasses M0 and cash-like equivalents, M2 adds current accounts, M3 adds longer-term bank deposits and similar financial assets, while M4 (and higher) extends to monetizable assets and investments on longer time-horizons. Broader phases are more inclusive, more complex, more diverse, and of lower mean liquidity. They therefore exemplify, most obviously, the Monetary Neo-Baroque. A tempting error would be to construe the monetary phases as ascending from the intuitively accessible into lofty technical obscurities. … Cash is cryptic. …

financial world do not have, and cannot have, any definite idea what money is. MΩ has no calculable determination. Far more importantly, at the other extreme, M0 is an advanced edge, and not a settled reality. It designates the intensive frontier of cash, commercial liquidity, or what money can do, as it has yet been historically encountered. In other words, it is problematic rather than theorematic, experimental rather than conceptual. Mx deranges all the formulas. We haven't seen anything yet. Crypto-currency is showing us that.

§5.653 — To refer to a neo-baroque is to invoke a decadent paradigm, in something like the Kuhnian sense.[301] Ptolemaic cosmology is the unsurpassable model. Crucially, it is indefinitely expandable. As it decays, epicycles accumulate, but never to a point of intrinsic lethality. There is no such point. The fundamental error is wholly retrospective. It would be no less mistaken to imagine the monetary neo-baroque dying from its own exploding complexity. Macro need only add epicycles. Nothing impedes such a development. Computers and professional hyper-specialization even facilitate it. Simplicity is for gold-bugs, and other primitives. If Macro's hypertrophic theoretical complexity appears increasingly magical – so much the better. Magic, as we have repeatedly seen, is functional. What matters to Macro – as institution, meta-institution, or regime – is primarily the credible illusion of understanding. That is where its authority lies. Macroeconomics must only pretend to a theoretical competence that is practically unobtainable. In this it epitomizes the socio-cultural status of expertise in progressive modernity, if not something far more general. Clerical authority has always rested on a pretention to mastery of that which is a mystery even to itself. Nothing new is to be expected there. Innovation arrives from outside.

§5.66 — Liquidity is valuable, uncontroversially.[302] It has a price. This is to say, reciprocally, that illiquid assets trade at a discount. Financial systems therefore automatically assimilate the concept of liquidity to that of risk, which configures illiquidity as negative investment quality. The essential – and innovative – macroeconomic contention is that liquidity preference, beyond a certain threshold, becomes excessive, malignant, and self-contradictory. Rather than returning to equilibrium, it feeds positively

[301] Thomas Kuhn outlined his catastrophic model of scientific history in The Structure of Scientific Revolutions (1962). He argues that empirical research is necessarily dominated by a conceptual framework which is comparatively resilient in respect to factual disconfirmation. When expressed at this level of generality, this is not a conclusion unique to Kuhn. It is one way that Kant's Copernican Revolution is expressed through the philosophy of science. Data is never unframed.

[302] Alfred Marshall's variable k defines aggregate liquidity through the ratio of broad money to economic output. While the formula acquires a certain rigor through its approximation to sheer tautology, both of its productive terms are notably elusive. Neither 'money' nor 'output' can be realistically conceived as simple, elementary, unambiguously measurable, or categorically delimited. Each is as plausibly captured by the processing of the other through k as by some supposedly primary factual apprehension. Macro, of course, fully – or at least very substantially – understands this. It takes perverse institutional (i.e. guild) pride in the inadequacy of its foundations, when inspected from the inside.

upon itself. Generalized investment aversion drains the pool of liquid assets, on a spiral into depression. Spending, then, is a social obligation, whose collective importance justifies suppression of private discretion. In this way, macroeconomics provides a specific model for the tragedy of economic liberty. This is its most profound counter-modernist theme. It is an argument translatable without remainder into the language of contradiction. On such lines, macroeconomics can be configured as an elaborated sub-plot within the critique of political economy initiated by Marxian historical materialism.

§5.661 — When configured in terms of mass social psychology, the thirst for liquidity expresses distrust, or negative confidence. Conceived economically, it is disinvestment. Conceived politically, it is dissent. Only liberalism, of the old type, would dissuade a regime from seeking to suppress it, and Macro – which is always Macro in power – means that liberalism is dead. The point can be made more strongly. Macro is the death of liberalism, in power.

§5.662 — All earnest pretension to 'counter-cyclical policy' notwithstanding, the systematic asymmetry is manifest. Politics tends to soft money. Governments – especially democratic governments – do not pass marshmallow tests. "In the long run we are all dead," Keynes famously quipped, and in doing so the voice of the state – now channeled by macroeconomics – was immediately audible. Delayed gratification was being explicitly re-modeled as a bourgeois vice. Created to 'manage' long-wave capitalist down-turns, and then to economic contractions of even minimal severity – its interventions scaled down by an order or magnitude to the pulse rate of (roughly) five-year business cycles – Macro tends to configure itself as the correction to capitalism in general. Globalization is deflationary, because it operates to control prices, through arbitrage. Technological efficiencies are an even stronger driver, in the same direction. The relation of macroeconomic stimulation to the capitalistic mechanization and globalization of production can therefore be understood as compensatory. Macro tacitly legitimates itself as an antidote to deep deflationary dynamics inherent to the modern economy. It is designed to make money soft.

§5.663 — While it requires a portrait of Macro – as a consummate regime – to see where we are, the picture takes us away from money, rather than toward it. Crypto-currency is the negative of all this.[303] It shorts political economy in general. The broad contours of a Micro Counter-Revolution are for the first time definitely indicated. Macro is essentially oriented against saving. In striking contrast, Bitcoin

[303] The realization that Bitcoin is an implicit threat to the entire edifice of the reigning macroeconomic order had been refracted, by end-2017, into Internet clickbait. "Dutch national newspaper urges people to sell all their Bitcoins as it undermines the government, could destabilise the economy and reduces the power of central banks."
https://www.reddit.com/r/Bitcoin/comments/7h9fkp/dutch_national_newspaper_urges_people_to_sell_all/

invents the 'hodler' who disdains short-term market interventions.[304] This is nothing less than the synthesis of a new bourgeois mentality or its substitute. A fierce re-animation of prudence accompanies the cryptic Micro insurrection. It understands, this time around, that it has dedicated enemies, true opponents, and not merely feckless villains indifferent to its virtues. Since Keynes, incontinence has been a cause, and then – almost immediately afterwards – a regime. All capacities for prudential self-protection outside state guarantees have been targeted explicitly for destruction. This is the framework within which money has been increasingly understood. Everyone should know, by now, what happens to 'hoarders' under socialism. Macro is only very slightly more subtle. Stigmatized liquidity preference is legible enough. The cultural importance of the intrinsic Bitcoin ideology follows from this. To 'hodl' is to hoard defiantly, in explicit recognition of the socio-political game being played. It is to save, not merely for the future, but for an impending revolution in the order of time. The value of Bitcoin, in this critical regard, is that of an option for liquidity preference that cannot be politically neutralized. It is the anti- New Deal. In other words, it is the Old Deal, but this time capable of protecting itself. No one is any longer relied upon to keep it. It keeps itself. That's what algorithmic governance means.

§5.664 — As money has 'evolved' the axis of inflation-deflation became ever more strongly determining. Money's dimension of variance through depreciation or appreciation is the carrier of its macroeconomic control function. As a good tool, it keeps the potential distractions of ulterior features to itself. Value is the message it is trained to focus upon. Also ever more, it seems ever thus. Yet 'inflation' is only superficially a trans-historical economic category. Over the past half millennium three distinct – if over-lapping – phases are identifiable. These can be related to the very different dynamics of monetary asset (bullion) glut, excessive (private) credit creation, and national macroeconomic relaxation. In each case there is an expansion of supply, which becomes inflationary when it results in a comparative abundance of money (relative to the general level of economic production). Such formal equivalence, however, offers little concrete guidance to the specific working of each monetary regime. Insofar as fractional reserve and then central banking can be seen to obey pre-existing economic laws, the insight is overwhelmingly retrospective. Neither innovation was discoverable through such compliance. On the pattern of the synthetic a priori, their necessity was found late. This – alone – can also be expected from what comes next.

§5.665 — Crypto-currencies initiate a new phase in the history of inflation. Bitcoin, crucially, structurally forecloses inflationary processes of the three dominant antecedent types. Its absolute abundance is rigidly constrained, fractional reserve multiplication is invalidated (as 'double spending'),

[304] To hodl is to hoard bitcoins, based on the presumption that they are radically undervalued relative to the eventual near-equilibrium level when they have come to denominate the principal terrestrial money system. The term seems to have been coined in late 2013, with the word freezing a comic misspelling. ("Hold on for Dear Life" is a subsequent humorous acronymic.) See: https://bitcointalk.org/index.php?topic=375643.0

and absolute 'policy neutrality' excludes macroeconomic laxity.[305] There is no tried-and-tested method of doing inflation with Bitcoin. This is not, however, to reach the end of the question. In the era of crypto-currency, appreciation-depreciation becomes ecological. It occurs between coins. Monetary pluralization, rather than monetary expansion, becomes the leading phenomenon.[306] After Macro, the deflationary dynamic reverts to a properly capitalistic – which is say Darwinian – distributed mechanism.

§5.7 —Nick Szabo begins his (2005) proposal for 'Bit gold'[307] with the remark: "A long time ago I hit upon the idea of bit gold. The problem, in a nutshell, is that our money currently depends on trust in a third party for its value. …" Even monetized precious metals, he notes, have involved trusted third parties in their validation. Worse still "you can't pay online with metal. Thus, it would be very nice if there were a protocol whereby unforgeably costly bits could be created online with minimal dependence on trusted third parties, and then securely stored, transferred, and assayed with similar minimal trust. Bit gold." Bit gold in this respect is indistinguishable from Bitcoin.

§5.71 — There is something at work here that the psychoanalytically-inclined might gloss as a *return of the repressed*. Since the triumph of paper over metal has been the central public narrative of 20th Century monetary history, the effect is unsettling – even uncanny. The metallic model was supposed to have been left behind. More specifically, the populations of 'sophisticated' or macroeconomically-managed and thus at least partially post-capitalist societies were supposed to have been *educated out of it*, automatically. Nothing more distinctly signals economic *primitivism* among such peoples than metalized wealth. Explicit lessons had seemed unnecessary, therefore. A return of gold from the economic margins looked no more likely than a restoration of Germanic Paganism.[308]

---

[305] Pierre Rochard describes Bitcoin's "non-discretionary monetary policy" as "asymptotic money supply targeting (AMST)".

[306] It should perhaps be noted that within the world of crypto commentary, this thesis is highly controversial.

[307] See: http://unenumerated.blogspot.hk/2005/12/bit-gold.html
Among the comments, there is much of interest to be found. Sampled glancingly:
"…you might want to check out http://www.bitcoin.org. It's a decentralized, P2P, cryptocurrency based on a proof of work algorithm."
"Congrats on inventing BitCoin …"
"Thanks for laying the foundation for bitcoin Nick …"
"One day, people will look upon this post as the actual genesis moment of Bitcoin."

[308] It would be tempting at this point to make a topic of *progressive complacency*, but in the present context it would be a digression too far. It need only be said that extravagant conclusions can easily be drawn from the realistic apprehension of ratchets. That there is *no way back* says much less about the resilience of the new order than is commonly supposed.

§5.72 — Among the attractions of *abstract metal*, none exceeds its inherited, intrinsic, adamantine resistance to discretion. Formalized negatively, with maximum concision, *Alchemy is impossible*.[309] Gold has no greater virtue than this. It precludes magic, as silver repels werewolves.[310] The replication of this characteristic within a digital simulation is Bitcoin's most basic achievement. It has realized homeopathic gold. Not a molecule of the original substance remains, yet the solution still delivers the cure. Fully-abstract gold has been modernity's obscure goal from the beginning. 'Invisible' credit money was its defective preliminary draft. Bitcoin, it turns out, is the true Philosopher's Stone.

§5.73 — Since Bitcoin has no central mint, it cannot generate revenue in a way strictly equivalent to seigniorage. It does, however, permit of a close analog. Early-stage miners of Bitcoin (or any related cryptocurrency) are able to accumulate substantial holdings with comparative ease, perhaps amounting to a significant proportion of the total (ultimate) stock. Similarly, early speculative investors can afford to take a commanding position in the currency during the early stages of introduction, when its price remains comparatively – and even, one might speculatively predict, *absurdly* – low. Of course, the introduction of speculative hazard into this analysis is already the pre-emption of a capitalistic justification. Once Bitcoin's prospects begin to be taken seriously, these early intimations of moral-political discomfort translate into acute concerns about the profound inequality of bitcoin distribution,[311] pitched upwards into vociferous fervor in direct proportion to the extent that such spiky stock holdings could now actually mean something. Yet even for the super-rich – defined narrowly for these purposes as those with personal assets exceeding the value of the entire bitcoin supply at present prices – optimizing a financial position in the crypto-currency at this early stage in its history involves a complex game. Since any attempt to monopolize the entire stock of coins would

---

[309] Much could no doubt be made of the fact that Isaac Newton was both an alchemist and the Warden of the Royal Mint. It is surely unnecessary, nonetheless, to insist that we see here something other than a simple contradiction. The poacher-turned-gamekeeper phenomenon is surely an important part of the story. Having paid serious attention to the possibilities of magical money-creation, Newton was well-placed to understand how the enemies of hard money think.

[310] Thus gold is hated among magicians. The antagonism is explicit. In the Macro era, the gold market offers an audience reaction to financial conjuration. It measures negative applause. "Jim Grant … describes the price of gold as the reciprocal of the credibility of central banks …"
See: http://kingworldnews.com/the-reason-for-our-unbroken-confidence-in-gold/

[311] A fully-monopolized monetary *stock* would correspond to a multiplication by zero. In *Libidinal Economy*, Jean-François Lyotard applies exactly this formula to the classical mercantilist valorization of unbounded bullion accumulation, which is thus exposed as a political-economic death drive. Comprehensive possession of a commercial medium is self-extinguishing. A powerful trading position does not extrapolate to absolute concentration. In monetary matters, there can be no completion of advantage. This 'paradox of wealth' is further accentuated in the case of Bitcoin, since adoption in this case has to be *coaxed*, under conditions never less than difficult, and – at least potentially – openly hostile.
http://www.thedailyriff.com/articles/the-paradox-of-wealth-776.php

suppress the value of BTC as a circulatory medium, it would be predictably self-defeating. The value of any currency has necessarily to be a more or less direct function of its social diffusion.[312] There can be little doubt that such calculations are in fact taking place, and their outcome – even, roughly, their 'equilibrium' – is among the crucial determinations of the bitcoin price. Currency monopolization – understood as ownership, rather than issuance, of the entire monetary stock – is an inherently paradoxical project.

§5.74 — It is easy to deride the notion of monetary 'backing' for its naivety (or in a more contemporary idiom 'pwnedness'). The idea has become a popular icon of duped thought. Its application to Bitcoin has therefore to be considered among the very weakest of criticisms, notable more as a symptom than an argument. There is – of course – nothing at all 'behind' (or 'backing') Bitcoin beyond the implemented Bitcoin protocol itself. This is not a unique feature. It merely makes Bitcoin post-classical ('modern') money. It is not being unbacked that makes it modern. Nothing was ever 'backed' beside deposit receipts. It is *the relevance of a question of backing* that carries the marker of modernity. Modernity in money is ecological coexistence with residual *promises to pay*. Naivety and cynicism are co-produced by it. Since the abolition of the gold standard, monetary 'backing' has been solely political. It rests upon the credibility of an issuing authority, which in turn rests upon more fundamental public perceptions of the durability, competence, and constrained malignancy of a regime.

§5.741 — The phased process of demetallization might appear to tell a story of cumulative monetary degeneration. Yet it would be a mistake to interpret this process as a dissolution of secure foundations. There is no type of money – however metallic – that can lay claim to an absolutely inherent value, extricable from a speculative assessment of its acceptability.[313] The desirability of a monetary medium cannot finally be grounded in its substantial properties, but only in the dynamic assessment of these properties, occurring within a market context. Its value is solely 'based' upon the system of scarcity it creates, insofar as this is latched onto by network effects. In consequence, money is essentially prone to ontological crisis – when it is discovered to be nothing in itself. Bitcoin accelerates the advance of monetary theory into cybernetic fundamentalism. It's turtles – or, more precisely, feedback dynamics

---

[312] A fully-monopolized monetary *stock* would correspond to a multiplication by zero. In *Libidinal Economy*, Jean-François Lyotard applies exactly this formula to the classical mercantilist valorization of unbounded bullion accumulation, which is thus exposed as a political-economic death drive. Comprehensive possession of a commercial medium is self-extinguishing. A powerful trading position does not extrapolate to absolute concentration. In monetary matters, there can be no completion of advantage. This 'paradox of wealth' is further accentuated in the case of Bitcoin, since adoption in this case has to be *coaxed*, under conditions never less than difficult, and – at least potentially – openly hostile.
http://www.thedailyriff.com/articles/the-paradox-of-wealth-776.php

[313] To quote Michael Goldstein (@Bitstein, from a tweet 2015/01/13): "I rarely see skepticism of Bitcoin that is not more generally just skepticism of money."

– all the way down. By philosophical analogy, the metallist theory of money corresponds to a pre-critical epoch, and the fiat era to an idealist efflorescence of elaborate, exhaustively constuctionist anti-realism. Cryptocurrency initiates a double-sided (transcendental realist) correction. Monetary value finds no ground outside the circuit, but the circuit is ontologically autonomous.

§5.742 — Currency[314] is money apprehended as a *means of payment*, flowing through transactions as a circulatory medium. Its principal virtue – liquidity – is a measure of how readily it is accepted in exchange for goods and services. 'Acceptability' is thus roughly synonymous with commercial value. Yet, when the acceptability of any currency is analyzed, it is found to depend primarily – if not exactly 'originally' – upon how widely it is accepted. However tempting it may be to dismiss such a nakedly circular definition as an absurdity, the formulation is deliberate, and informative. The acceptability of money is irreducibly self-referential. Money is acceptable in any particular case only because it is acceptable in general, while generality is a cumulative product of particularity, and nothing besides. The nonlinearity is essential, rather than accidental, and cannot be resolved into anything more fundamental. This is evidently a problem of the 'chicken-and-egg' type, characteristic of positive feedback dynamics. Thus, as previously noted (perhaps obsessively), the virtuous circle of liquidity translates, without remainder, into a display of network effects. The utility of a network, to each individual user, grows superlinearly with the number of users. With currency, as with all systems that generate positive returns to scale, 'nothing succeeds like success', and there is ultimately nothing to success besides. There is no basis of value to be excavated beyond or beneath its own self-reinforcement. The supreme, self-grounding virtue of *acceptability* is thus practically revealed. Conceptually, acceptability is integrative, since the functions of money as a store of value and as a unit of account can be gathered under it (distinguished only formally, rather than substantially). We enter the cybernetic abyss, without transcendent ground. The succinct account of this dynamic provided by Koen Swinkels cannot easily be improved upon:

Ultimately the only thing that matters in people's decision to use bitcoins as a medium of exchange is their expectation that enough other people will accept it as payment in the future. That alone is enough basis for people to buy bitcoins now and to invest in the bitcoin infrastructure now. […] The circularity involved in the argument is unmistakable but unavoidable and, according to the bitcoin enthusiasts, unproblematic. That's just the thing about a good that is used as money or is expected to be used as money in the future: people value the good because they think that enough other people will value it. The circularity is just the network effect in action.[315]

[314] A currency (from Middle English: *curraunt*, "in circulation", from Latin: *currens*, *-entis*) is money circulating as a medium of exchange.

[315] See: http://www.philosophyofbitcoin.com/2014/07/bitcoins-store-of-value-paradox.html

§5.75 — Since Bitcoin advocacy is indissociable from claims about the quality of money, it is propelled into a collision with Gresham's Law, as popularly – and quite adequately – summarized by the maxim *bad money drives out good*. Gresham-effects can be easily recognized in modern life. Given two cash notes, one pristine, the other crumpled, stained, and taped together, which would one expect the holder to be inclined to part with first? In an earlier monetary era, characterized by widespread coin-clipping – rather than germ-saturated paper – the economic significance of such decisions was more substantial. As exemplified by such examples, the most intuitively compelling application of Gresham's Law is to physical cash. The classic archaic case concerns two coins of identical nominal value, but differentially clipped. The negative comparative appeal of the 'short' coin – which any holder wants as soon as possible to be rid of – accelerates its *currency*. A 'pass-the-parcel' dynamo is envisaged. Implicit within this model is the proposition that the disposal, rather than acceptance, of currency is the primary driver of its circulation. There is a crucial irony – which we will return to in its other guises – that *the spontaneously-concerted attempt to shed bad money looks indistinguishable from an illustration of good money*, especially when hoarding is conceived as an anti-social economic vice. Money is most stimulative when it is least wanted.[316] Yet this assumption requires a peculiar inversion. Since even minimal acceptability is non-mandatory under ordinary economic conditions, we can be confident that it is in fact the 'good' coin that propels the circulation of the 'bad' one, by sustaining the standard of value which the inferior instance parasitizes. The tacit calculation involved in every acceptance of a bad coin includes the question as to whether it still suffices to *pass* as a acceptable money.

§5.8 — Whether history 'in general' is anything other than the history of money remains an open question. Certainly, the distinction between 'history' and 'pre-history' seems to have been decided by monetary innovation. The earliest digital recordings are accounts.[317] In the beginning was the registry. If this distribution of emphasis seems unbalanced, the fact that – in our own time – a distributed ledger manifests primarily as a monetary innovation tends, nevertheless, to vindicate it. Commentary in the

---

[316] Gresham's Law identifies the attractiveness of a monetary medium as a source of commercial friction. Monetary quality, under the most straightforward construction of the argument, poses an intrinsic obstacle to spending. Money is thus already modeled, implicitly, as *ideally repulsive*. In this regard, Keynesian Macro appears as a higher Greshamism. Good and bad switch places. Or rather, the good money people would prefer to keep is denounced as an evil temptation to 'cash preference'. It is the bad money, intrinsically motivating its own disposal, which now counts as 'good'. A slave revolt in monetary theory has then taken place.

[317] See Denise Schmandt-Bessera, *The Earliest Precursor of Writing* (1977 / 06): "Evidently a system of accounting that made use of tokens was widely used not only at Nuzi and Susa but throughout western Asia from as long ago as the ninth millennium BC to as recently as the second millennium."
http://en.finaly.org/index.php/The_earliest_precursor_of_writing

"Bitcoin is about much more than money" vein, while copious, also comes later.[318] The monetary model sets the matrix.

§5.81 — A bitcoin, or part of a bitcoin, is a number of numbers, or several. In this it reproduces an abstract structure that is essential to the nature of money, in any of its variants, although realized at very different degrees of formalization. The semiotic complexity of money is expressed by a multiplicity of numerical dimensions. (Money not only quantifies, it quantifies multiplicitously.) Even prior to the introduction of *allocation*as a topic, monetary numbers divide by signification and designation. They function arithmetically as counting numbers and indexically as registry numbers (indices). The distinction is illustrated by the coexistence of a denomination number and a serial number on every bank note. The final term in the semiotic triad – the allocative number – corresponds to a tallying of bank notes, for instance – most concretely – through their bundling into 'bricks'. These dimensions are primeval. Yuval Noah Hariri writes (in *Sapiens: A Brief History of Humankind*, p.182): "The first coins in history were struck around 640 BC by King Alyattes of Lydia, in western Anatolia. These coins had a standardized weight of gold or silver, and were imprinted with an identification mark. The mark testified to two things. First, it indicated how much precious metal the coin contained. Second, it identified the authority that issued the coin and that guaranteed its contents." The coin bears an index of composition and a sign of credentials. The third semiotic dimension is added in a counting house, and introduces – from the beginning – the *ledger*.

§5.82 — Every commercial transaction involves a conversion into numbers. There is no primordial difference between monetary circulation and *digitization*, recognized as *the*historical process. In its narrower, electronic sense, however, the digitization of money does not date back very far. The first electronic money precedes Bitcoin by no more than half a century. Precursors are retrospectively identifiable, including charge coins, charge cards, 'charga-plates', and air travel cards. Western Union began issuing charge cards to frequent customers as early as 1921, but the runaway electronic

[318] Morgen E. Peck writes: "… money is only the first, and perhaps the most boring, application enabled by Bitcoin technology." http://spectrum.ieee.org/computing/networks/the-future-of-the-web-looks-a-lot-like-bitcoin

'derealization' of money is a far more recent phenomenon.[319] The first credit card[320] – accessing a bank account by means of a plastic identification document – was the BankAmericard, launched in September 1958 (and renamed 'Visa' in 1977). It took another eight years for the system to be extended beyond the United States (to Britain, with the 'Barclaycard', in 1966). The spread of electronic banking outside the English-speaking world was far slower still. Widespread adoption of the new monetary medium in Continental Europe, for instance, did not take place until the final decade of the 20thcentury. Most of the world skipped this stage of monetary evolution altogether.

§5.821 — *Electronic monetary transfers* – as required by credit cards – are not yet an *online payment system*. The former involves electronic settlement, but not yet digital cash.[321] Electronic bank credit operates exclusively between *trusted parties*. The cash-like aspect of the transaction takes place offline, between the cardholder and the goods or services provider. Even here, some basic characteristics of cash are sacrificed, most notably anonymity. It is 'cash' in this reduced sense that is translated online by the first consumer-level digital money services, exemplified by PayPal.[322]

---

[319] Conceived as a popular cultural theme, the guideline to the plastic phase of money was *invisibility*. In this respect it evidences a teleological model, defining an axis of progress. Monetary improvement is sublimation, or dematerialization. In accordance with classical precedent, finality is identified with the pure idea, beyond all contamination by, or compromise with, particular substance. As previously noted, something more than a convergence with mathematical Platonism is at work here. The history of money – whether actual or fantastic – does not draw upon idealism as an extrinsic inspiration. Rather, it idealizes practically, and even preemptively. Elimination of friction – as implicit and later explicit goal – serves as a convenient proxy for the monetary ideal. Keynesian derision of the "barbarous relic" – the primitive *lump sum* – is once again the critical reference. Progress – conceived implicitly as financial dematerialization – is projected into space as a ripple pattern. Differential adoption rates and patterns of diffusion mark out stages of development, organized by a definite *telos*(distinguishing advanced from primitive money). According to this schema, at *the end of money*, the transaction coincides exactly with its Idea. The medium is then nothing. If the notion of *a direct private relation without frictional mediation* carries certain historic-religious associations, these are probably not coincidental.

[320] The term 'credit card' seems to have first been employed by Edward Bellamy, in his utopian-socialist novel *Looking Backward* (1887).

[321] Marc Andreessen says of Bitcoin, in a Washington Post interview (May 21, 2014): "…if we had had this technology 20 years ago, we would've built it into the browser. […] E-commerce would've gotten built on top of this, instead of getting built on top of the credit card network. We knew we were missing this; we just didn't know what it was. There is no reason on earth for anybody to be on the Internet today to be typing in a credit card number to buy something. It's insane …"
http://www.washingtonpost.com/blogs/the-switch/wp/2014/05/21/marc-andreessen-in-20-years-well-talk-about-bitcoin-like-we-talk-about-the-internet-today/

[322] PayPal was created from the merger of Confinity (founded in December 1998 by Ken Howery, Max Levchin, Luke Nosek, and Peter Thiel) with X.com (founded in March 1999 by Elon Musk). The new company was established in March 2000, acquiring its name the following year. PayPal went public in February 2002, in an IPO that generated over $61 million. The company was sold to eBay in July of the same year for $1.5 billion. (The

§5.83 — It was not the personal computer that set the frame for the next stage of money's technological evolution, but the mobile phone. Within this new epoch of consumer electronics, 'personalization' is intensified, through heightened communicative-orientation and the massive distribution of computational capability.[323] It is easy to miss the full complexity of the mobile phone as a technological nexus. Not only does it serve as a telecommunications and Internet-access device, but also as a scanner, and a personal identity hub. In combination, these features enable convenient, efficient, and passably secure monetary transactions. The serendipitous contribution of an in-built camera to the mobile phone's function as a monetary platform is especially worthy of note. A facile photographic shot closes the transaction. The era of the bar-code thus passes into that of the QR-code.

§5.831 — The age of mobile payments dates back only to 2007. In that year, Safaricom and Vodacom, the largest mobile network operators in Kenya and Tanzania respectively, released their M-Pesa mobile-phone based finance application, developed by Vodafone. 'M-Pesa' abbreviates 'mobile money' in hybrid tech-jargon and Swahili. The application was designed to support elementary banking services on wireless telecommunications, in drastically under-banked societies. It enabled monetary exchanges between users, with the additional capability to facilitate microfinance credit. Anybody with identity certification (such as a national ID card or passport) could use M-Pesa to deposit, withdraw, or transfer money through their mobile device. Its rate of adoption exceeded all expectation, resulting on social,

---

resulting Musk and Thiel fortunes have been among the most nourishing seed-beds of 21st century capitalism.) The extreme synergy between eBay's online market-making business and PayPal's secure digital payment service propelled its initial growth, first in the US, then through eBay's international business, and finally beyond eBay. PayPal was spun-off from eBay in July 2015, following the firm recommendation of hedge fund manager Carl Icahn. It began to accept bitcoin in September 2014, announcing partnerships with Coinbase, BitPay, and GoCoin. While PayPal has been rewarded by the market for its pioneering role in facilitating financial transactions over electronic networks, its limitations are severe, and in the age of cryptocurrency increasingly obvious. Its users are entirely unprotected from the company's radical discretion, and receive no exit benefits from the service in respect to the national-financial regime in which they operate. Essentially, PayPal adds a new 'trusted third party' to the financial ecology, and one of minimal autonomy. Nothing very much has been disrupted by it.

[323] The resonance between *mobile* consumer technology and *portability* as an essential monetary quality cannot be coincidental to the emergence of mobile currency. A desktop wallet is patently inconvenient. By its abstract nature, money is destined to eventual convergence with the communicative situation in general, which it *tends* to haunt as an accessible semiotic dimension. Wherever speech can occur, the potential for contractual execution will finally follow. Only in this way is *Homo economicus*completed. At the confluence of these currents lies the inevitable formula: *Money is speech*. It not only assumes, in the Anglosphere cultural context, informal and formal constitutional protection in the cynical culmination of liberalism. The claim extends further – into identity with *the claim* as such. Money – the pure power of acquisition – seizes for itself the mantle of realizable *logos*. The conceptual fusion of the *smart contract* is reversible. Transactions can be augmented by machine intelligence because intelligence is inherently transactional. Minds and market-places tend to convergence.

cultural, and commercial success on a now already legendary scale. From its take-off point in East Africa, the service was subsequently expanded into Afghanistan, South Africa, and India, reaching Eastern Europe in 2014. It has been in China, however, that the new fusion of money and telecommunications has developed most explosively. China's mobile payment market has been opened by its Internet giants Alibaba and Tencent. Up to late 2015, Alipay dominated, accounting for over two-thirds of mobile purchases by value. Tencent's competitor system, based upon its WeChat[324] social media application, consolidated its position through a highly-successful marketing campaign themed by digital emulation of traditional 'red-envelope' monetary gifts. By the first quarter of 2017, Alipay and WeChat between them were servicing 94% of the country's mobile payment market. Chinese late-mover advantage has enabled the country to leap-frog plastic, transitioning directly from paper to wireless. By early 2017, US online payments amounted to scarcely 2% of the Chinese figure (which had reached the equivalent of US$8 trillion).

§5.84 — The story of electronic money is not exhaustively subsumed into that of banking. In has various quite separate lineages, of greater and lesser independence. One of the most important of these passes through online multi-user environments and games. The fictional quality of in-game monetary systems has shielded them from regulatory scrutiny, to a degree that cannot easily be philosophically defended. They thus open a zone of special interest in regards to the ontology of money.[325] What is the relation of 'real' money to simulated money? Virtual currencies, such as the Linden Dollars (L$) of *Second Life*, made this question ineluctable. If online 'pretend' currencies had an exchange value denominated in offline 'real' currencies – as they soon did – how solid could any ontological discrimination between the two be? It began to dawn upon commentators that a new age of private currency issuance had been surreptitiously initiated. It is perhaps a matter of mere historical contingency that far more consequential developments have not yet been catalyzed in this zone. There are few obvious limits to what might have come.

§5.841 — The industrialization of virtual currency production in the crypto-epoch was partially anticipated by the phenomenon of 'gold farming' in the world of MMORPGs (or Massively Multiplayer Online Role-Playing Games). Many of the most popular MMORPGs permit trading in items of in-game value. For instance, a special weapon acquired at the cost of much (in-game) effort and peril, and therefore scarce enough to be precious, might be surrendered by one avatar to another in exchange for an out-of-game payment between their respective players. Such arrangements called out for economic

---

[324] The scale of WeChat (微信, Wēixìn) can be hard for those outside China to appreciate. With over a billion regular users, the application is truly ubiquitous. WeChat messaging accounts for over a third of the country's (massive) mobile phone usage.

[325] Given the striking philosophical importance of (ludic) virtual currencies, the social under-development of the problem is remarkable. An obvious exit ramp from the Macro financial regime has been almost entirely ignored.

rationalization, through specialization, concentration, and Internet-enabled geographical labor arbitrage. China's business renaissance during the reform-and-opening period coincided with the emergence of this opportunity, and its new entrepreneurs moved nimbly to take advantage. Tedious game play was quickly transformed into commoditized labor, as cheap, capable, Chinese youngsters were organized by upstart businesses to undertake grueling virtual activities. Such 'gold farms' thus functioned as exchanges. Through them, game currencies could be laundered into 'real' money. A Möbian economic circulation now crossed seamlessly between the virtual and the actual.

§5.85 — Perhaps not finally, but at least additionally, and decisively, there is the lineage of cryptocurrency innovation itself. It arose from the application of public key cryptography (PKC) to the specific problem of monetary transactions. The work of David Chaum, in the early 1980s, was especially decisive in this regard. Chaum's 1983 paper on 'Blind Signatures for Untraceable Cash' was a landmark advance.[326] The problem it sought to solve was specific to the meaning of cash. Digital money is comparatively straightforward. It requires only the secure transmission of bank account details across the Internet, and appropriate modification of balances. Cash is more difficult (in rough inverse proportion to its superior facility). It has to operate like a bearer bond, making no reference to the identity of its holder. A cash payment is nobody else's business.

§5.851 — Blind signatures, like cash, had a pre-digital instantiation. They required only carbon paper, envelopes, and rigorous method.[327] Everything was dependent upon procedure.

§5.852 — The basis for strong digital signatures was established by asymmetric or 'public key' cryptography in the mid- to late-1970s.[328] The further step to digital blind signatures was required to make these cash-like. Already with PKC there is suggestive 'blindness'. It enables any particular private

---

[326] Chaum, David — 'Blind Signatures for Untraceable Cash', Advances in Cryptology Proceedings 82 (3) (1983) http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF

[327] For the purpose of analogy, Chaum notes (in his Blind Signatures paper) that an off-line anticipation of the procedure is provided by certain ballot validation systems. In these, too, identification (of a legitimate voter) has to be combined with the preservation of anonymity. This can be achieved by enclosing the ballot in a carbon paper sheath that certifies the voter's credentials. An election official signs this envelope, transferring the signature to the unseen ballot inside. The sheath is then discarded, leaving the authenticated but anonymous ballot to be safely cast. Neither signer nor eventual vote-counter are able to connect the 'message' (vote decision) with the individual who transmits it, and who has nevertheless been securely certified to do so.
In the paper, Chaum re-describes the system algebraically to identify the algorithm:
(1) Provider chooses x at random such that r(x), forms c(x), and supplies c(x) to signer.
(2) Signer signs c(x) by applying s' and returns the signed matter s'(c(x)) to provider. …
(3) Provider strips signed matter by application of c', yielding c'(s'(c(x))) = s'(x).
(4) Anyone can check that the signed matter s'(x) was formed by the signer, by applying the signers public key s and checking that r(s(s'(x))).

[328] Asymmetric cryptography is the principal topic of the subsequent chapter.

key to be recognized without ever being seen. A public key is able to validate a private key without displaying it. This already provides a strong analogy for the function of signatures, which are ideally identifiable without being reproducible. In the digital arena, where the ability to authenticate seems more obviously bound to a technical option to forge, the near-paradoxical demand placed upon traditional signatures becomes more evident. Chaum notes further that signatures are reliable only if conserved. An additional near-paradoxical demand placed upon them is that they cannot be repeatedly copied.[329]

§5.853 — Chaum's insight was properly transcendental-philosophical, or diagonal. It achieved the apparently impossible, translating cash into Cyberspace, by conceptually breaking the false tautology of authentication and identification. The new diagonal creature thus released was the verified but anonymous holder of communicable virtual property. Something like a prototypical cryptocurrency is thus initiated.[330] Chaumian cash, or 'ecash' was actualized as DigiCash in 1989, which survived into 1998.

§5.854 — Chaum has a reputation for prickliness which intrudes into the story-line, at least insofar as it led him to turn down an offer of US$100 million from Microsoft to incorporate DigiCash into Windows 95. It is difficult not to see history fork here. An alternative history exists in which cryptocurrency was mainstreamed by the late 20thCentury. With cryptocurrency having missed this early turn-off into actuality, the types now arriving are almost certainly harder, and more socially abrasive, than they might have been. It seems as if the Ultras booked a pre-emptive win.

§5.86 — Arvind Narayanan and Jeremy Clark helpfully decompose cryptocurrency – as initiated by the Bitcoin synthesis – into three functional modules, which can be traced back along distinct technical lines. Crossing the threshold into cryptocurrency requires bringing together a resilient decentralized registry, secure value-tokens, and a gauge of computational contribution, in a fully-converged operational singularity.[331] Within this combination, each thread exposes its complicity with an

---

[329] In Chaum's algebraic formulation, even with s'(c(x1)) … s'(c(xn)) and choice of c, c', and xi, it is impractical to produce s'(y), such that r(y) and y≠xi.

[330] Chaumian cash falls short of a full cryptocurrency. It is not, for instance, denominated in its own currency units. (No mechanism for currency production is involved.) Its deficiencies do not stop there. Reliance on banking institutions remains undiminished. Perhaps most defectively, it is only able to support a single monetary denomination, of arbitrary scale, but then unchangeably. Host currency inflation would therefore eventually degrade it. In Chaum's words: "The critical concept is that the bank will sign anything with its private key, but anything so signed is worth a fixed amount, say $1."

[331] See: Arvind Narayanan and Jeremy Clark, 'Bitcoin's Academic Pedigree' (2017). Bitcoin is a triadic dynamo. "In bitcoin, a secure ledger is necessary to prevent double spending and thus ensure that the currency has value. A valuable currency is necessary to reward miners. In turn, strength of mining power is necessary to secure the ledger. Without it, an adversary could amass more than 50 percent of the global mining power and thereby be

abstracted realization of money, in one of its three ineliminable semiotic aspects. The index of value-storage, the sign of accountancy, and the token of actual payment (i.e. exchange), are the exhaustive, irreducible, indispensable, and mutually-dependent features of any functional monetary order.

§5.861 — The early 1990s saw the conceptual innovation of robust (or 'append-only') data-structures capable of providing secure ledgers. Such structures introduce a *gradient*. They make data-bases sedimentary, and time-like.[332] The past is protected against revision, as a type of artificial, hard or ideal memory. Irrevocable commitments were thus digitally supportable. Since backing out of an executed deal is the typical mode of double-spending, a capability for the hardening of commitments has special relevance to the implementation of cryptocurrency. Indeed, its importance is such that there is a tendency among much Bitcoin commentary to reduce the innovation to 'the blockchain' which is itself then summarized as a distributed, revision-resistant ledger. Remaining within the Narayanan and Clark schema, the technological lineages leading to the emergence of such decentralized chronotypic databases are themselves susceptible to further triadic classification. Specifically, they assemble advances in the fields of linked time-stamping, Merkle trees, and byzantine fault tolerance.

§5.8611 — Even before timestamps were conceptually, and then practically, linked, a *timestamp* was already a 'trusted timestamp' if it was anything. Verifiable dating of digital documents poses a problem closely analogous to that of digital money, brought to a point of criticality by the ease of perfect replication. In both cases, initial solutions involved procedures of formal vouching by trusted third parties. For timestamps, the role of supervised banks is taken by Time Stamping Authorities (TSAs).[333] Public Key Cryptography is employed to render time-stamps indelible – resistant to modification by anyone accessing the document in question, including its creator.

---

able to generate blocks faster than the rest of the network, double-spend transactions, and effectively rewrite history, overrunning the system. Thus, bitcoin is bootstrapped, with a circular dependence among these three components."

[332] Narayanan and Clark capture the philosophical essentials well. "In a simplified version of Haber and Stornetta's proposal, documents are constantly being created and broadcast. The creator of each document asserts a time of creation and signs the document, its timestamp, and the previously broadcast document. This previous document has signed its own predecessor, so the documents form a long chain with pointers backwards in time. An outside user cannot alter a timestamped message since it is signed by the creator, and the creator cannot alter the message without also altering the entire chain of messages that follows. Thus, if you are given a single item in the chain by a trusted source (e.g., another user or a specialized timestamping service), the entire chain up to that point is locked in, immutable, and temporally ordered."
https://queue.acm.org/detail.cfm?id=3136559

[333] As the Internet Society remarks in 2001, in proposing the RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol: "In order to associate a datum with a particular point in time, a Time Stamp Authority (TSA) may need to be used. This Trusted Third Party provides a 'proof-of-existence' for this particular datum at an instant in time."
See: https://tools.ietf.org/html/rfc3161

§5.86111 — Linked timestamping draws primarily on work by Haber and Stornetta, dating back to the beginning of the 1990s.[334] This work was directed towards secure notarization, which is to say the verification – within a digital environment – of a document's historical existence, with special reference to questions of *priority*. A facility of this kind has obvious relevance to legal documents, such as contracts and intellectual property claims. Linking timestamps adds dynamic to the procedure, by extending it to digital entities undergoing successive modification, such as changing inventories, and accounts. At each (discrete) stage of transformation, an additional timestamp is signed, or (in later versions) hashed, constituting a *chain*, pointing into an increasingly edit-resistant past. Each timestamp in the chain envelops the preceding series. It thus establishes public *order*, or absolute succession, in which the past is uncontroversial, and secure. As Satoshi Nakamoto notes in the Bitcoin paper, "Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it."

§5.86112 — A series of linked timestamps is already, at least in embryo (or larva), a 'block-chain'. The stamps operate as irreducible moments, whose order is settled (immanently) by embedding. Their time is sheer order, without cardinality. Any timestamping system nevertheless inherits a time-keeping procedure, amounting to a fully-functional calendar, whose granulated 'dates' it competently codes. Unix time is the most widely applied system of this kind. Bitcoin adopts it.[335]

§5.86113 — Taking timestamping into trustlessness was a development that had to await Bitcoin.[336] While linked timestamping provides the basic architecture for secure (edit-resistant) ledgers, their robust decentralization depends upon additional cryptographic advances, supporting validation, compression, and consensus.

§5.8612 — Decentralization of the ledger requires massive multiplication, and thus an effective method of compression. Only in this way does it become tractable to distributed, modestly-sized nodes. The crucial computer science innovation in this regard is the Merkle Tree. The capabilities drawn upon date

---

[334] See: Haber, S. and Stornetta, W.S. 'How to time-stamp a digital document' (1991)

[335] Unix time counts forwards, in seconds, from 00:00:00, January 1, 1970, (a Thursday). It ignores leap seconds, treating the length of each day as 86,400 seconds. It therefore gradually drifts from Universal Time.
When encoded in 32-bit format this time system reaches (Y2K-type) crisis on January 19, 2038. This poses no direct threat to Bitcoin, which employs a fully future-competent 64-bit Unix time code.
https://en.wikipedia.org/wiki/Unix_time

[336] See (for e.g.): Bela Gipp, Norman Meuschke, and André Gernandt, 'Decentralized Trusted Timestamping using the Crypto Currency Bitcoin' (National Institute of Informatics Tokyo, Japan, 2015)
https://www.gipp.com/wp-content/papercite-data/pdf/gipp15a.pdf

back over a decade before linked timestamping, with Ralph Merkle's original hash tree patent was granted in 1979.[337]

§5.86121 — Hashes are economizations.[338] They reduce the cost of checking, by securely summarizing units of data, and therefore cheapen the process of verification. Any radically decentralized (open fully-peer-to-peer) network is necessarily trustless, since it connects strangers in the absence of validating authorities. Consisting of both massively redundant distributed databases and numerous untrusted nodes, *checking* is at once especially inconvenienced, and especially necessary.

§5.86122 — As their name suggests, Merkle Trees map an order of proliferation, typically – though not necessarily – modeled by successive bifurcation. Their function, however, is the precise inverse of tree-like exponential growth. A Merkle Tree works *towards* its roots, in increments of convergence. As users proceed down the tree, hashes of network content are bundled, recursively, into ever more comprehensive groups. The 'root' or (confusingly) 'top hash' over-hashes the entire tree. It thus serves as a concise compendium for the entire network, against which the hash of any file (or block) can be conveniently checked. Recursive hashing – hashes of hashes of (ever more) hashes – is the principle of the 'tree'.

§5.86122 — Cryptographic hashing has a peculiarly intimate[339] relationship with cryptocurrency, and thus with money as such in its emergent characteristics. This is in part, and primarily, because the hash is the privileged semiotic of singularity – to the extent that 'hash collision' is calamitous for it. Hashing therefore tends to affinity with the allocative or economic sign.

§5.8613 — As differences accumulate in a decentralized database, it tends naturally to divergence. No authoritative tribunal exists in which to resolve disagreements. Not only is trustlessness the default, but the space for malicious deception is not easily limitable. Since contracts are *agreements*, a decentralized system without trusted third parties is a challenging place to do business of any kind. Those special – if typically momentary – contracts which are monetary transactions are no less profoundly problematized than any other. More specifically, insoluble controversies over their unique execution would generate double spending problems, which no money system could tolerate. Without

---

[337] Ralph Merkle's hash-tree patent (US4309569A) is titled a "Method of providing digital signatures". Its abstract (in full) runs: "The invention comprises a method of providing a digital signature for purposes of authentication of a message, which utilizes an authentication tree function of a one-way function of a secret number." The description that follows expands upon its potential applications. "The present invention has been described with respect to authentication of signatures. However, its use is not limited to signatures. It may be used to authenticate a piece of information in a list of information, or one item in a list of items."
The patent can be accessed online at: https://patents.google.com/patent/US4309569

[338] See **§2.31**

[339] See **§3.422-4**

an effective *consensus mechanism*, the basic compatibility of commerce with radical decentralization is plausibly questionable.

§5.86131 — The general solution space for dissensus and double-spending problems in decentralized systems has been explored under the name of *Byzantine fault-tolerance* (BFT).[340] This measures the resilience of a network in respect to the operation of treacherous nodes. 'Byzantine' references the Byzantine Generals Problem, which was conceptually formulated in the late 1970s, although the name itself is a few years more recent.[341] The Byzantine Generals Problem belongs to a larger class of 'Generals Problems' in computer science, all of which address questions of coordination between independent networked modules or agencies, especially when complicated by trustless communication. The joint work of Leslie Lamport, Robert Shostak, and Marshall Pease is the crucial reference.[342]

§5.86132 — When apprehended teleologically, which is to say *given Bitcoin*, the Byzantine Generals Problem and Proof-of-work fit together like lock and key. Current discussion thus tends to scramble the two together, with the term 'Byzantine Fault Tolerance' serving as something close to a synonym for proof-of-work validation. Satoshi Nakamoto's engagement with the Byzantine Generals Problem inaugurates the genre.[343] The consequence is an obscured synthesis. Something is brought together by Bitcoin Byzantine Fault-Tolerance whose original geneses were quite distinct.

§5.86133 — The central concern of Lamport, Shostak, and Pease is to determine the cost of reliability in insecure systems. Since fault-tolerance – in their estimation – is attained only through redundancy, it has a price determined by the measure of necessary message duplication. The message validation algorithm they propose requires that at least two-thirds of the communicating nodes are trustworthy (without – of course – knowing in advance which ones). No appeal is made to proof-of-work credentials, or in general to any kind of intrinsic message credibility.[344]

§5.86134 — Beyond their function as a technical designation, the Byzantine Generals mark the emergence of a rare modern myth. They plot an assault upon a city, under conditions that typify the

---

[340] See **§4.08**+

[341] The Byzantine Generals Problem was immediately preceded According to a comment appended to the 1982 article, the 'generals' confronted by this archetypal network coordination problem were Chinese, and then Albanian, before finally being identified – for reasons of diplomacy – as Byzantine.
See: https://www.microsoft.com/en-us/research/publication/byzantine-generals-problem/

[342] See in particular Lamport, Leslie; Shostak, Robert; and Pease, Marshall; 'Reaching Agreement in the Presence of Faults' (April 1980) and 'The Byzantine Generals Problem' (1982).
https://www.microsoft.com/en-us/research/uploads/prod/2016/12/The-Byzantine-Generals-Problem.pdf

[343] See **§4.08**

[344] Some qualification of this claim might be suggested by the fact that in their 1982 paper, Lamport, Shostak, and Pease entertain the possibility that secure digital signatures could contribute to Byzantine solutions.

'nomad war-machine' in its philosophical acceptance – that is, *dominance of external relations*.[345] Having no interiority, the attackers have no default information security. Their domain is trustless, and primordially disunited. Integration is never given, but only strategically produced, as a precarious synthesis. It is this condition that the word 'Byzantine' is hijacked for, irrespective of the historical incongruity involved. The attack is – strictly – a critique. We have then, in the Byzantine Generals Problem, the mythical image of an assault upon centralization, unity, and interiority, staged from the Outside. Computer science, and later a far wider audience, is drawn into dramatic sympathy with this attack, and its 'Byzantine' heroes. In tackling the problem, or watching it tackled, we root for the unnamed city to fall.

§5.862 — Under even modest techno-historical scrutiny, cryptocurrency divides within itself, or doubles. Beside the major topic of money-production is revealed a minor (and inward-turned) twin. Cryptocurrency has its own – additional – use for money, which is to say for itself, intrinsic to its possibility. It folds upon itself essentially. While making money – in multiple senses – it also makes *of* money a new, specific machine-part. There are things it needs doing which will not be done unless rewarded. Thus the initial return on the issuance of money – *seigniorage* – is allocated by Bitcoin to the maintenance of its own decentralization.[346]

§5.8621 — Only by way of money in its minor sense – i.e. as the mining compensation token – does money in its major sense undergo practical redefinition as *an automatically self-sustaining decentralized system*. The path of money production is shaped by the protocol in such a way as to spontaneously reinforce those user behaviors the system depends upon. So tightly is this incentive mechanism constructed that all bitcoins originally reward Bitcoin maintenance, while also stripping Bitcoin maintenance of discretion, by integrating it rigorously into the process of mining. There is nothing a bitcoin miner *can*

---

[345] "As for the war machine in itself, it seems to be irreducible to the State apparatus, to be outside its sovereignty and prior to its law: it comes from elsewhere." (Deleuze & Guattari, *A Thousand Plateaus*, p.352)

[346] It might be asked: *Was it not always necessary to pay gold-miners – or at least for gold-mining – as also for work in the mint, or the central bank? Did not money, then, always involve a minor internal digression or auto-productive reflex? What is really new here?* Raising this question is potentially informative, since it tends to isolate the cryptocurrency innovation. The incentive system at work in Bitcoin substitutes for monetary authorities. The only forerunner is to be found in primary precious-metal production, in which – crucially – the miner is rewarded immediately and automatically for industrial activity. Neither work contract nor marketing is necessary. Mining, of this kind, *produces money*. In the case of Bitcoin, all money – without exception – is mined, originating as property of the miner. Bitcoin is not, however, reducible to simulated gold. Bitcoin mining, unlike its concrete precious-metal predecessor, is also, simultaneously, minting, or monetary validation. A functional analog of the assay is built into the mining process, integrally. Its cycle produces trust, rather than drawing upon it. What makes it good money is made part of the way it makes money. This seamless loop is its essential innovation, synonymous with what *cryptocurrency* means.

do to sustain Bitcoin beside mining bitcoins. Sheer industrial effort, alone, is rewarded, and that has been made enough.

§5.8622 — It is particularly important to note that bitcoin mining rewards make no payment for loyalty, as compensation for non-defection. The miner is not in any respect a *trusted official*. The relation between money and trust has been fundamentally re-ordered. It is rather, now, that the miner makes bitcoins trustworthy through an activity which demands no trust whatsoever. The historical passage, as previously remarked, is from the consumption of trust to its production. §5.8623 — Currency units denominate incentives. There is nothing notably novel in this insight. Making *incentive engineering*inherent to currency production, however, proved a decisive technological break. Bitcoin initiates the epoch of cryptocurrency, strictly speaking, by structuring its protocol as a game. This is the sense the *token* now carries. Besides providing money, it directs those behaviors specifically required for its social implementation. The positive cybernetic loop here is conspicuous, and remarkably ingenious. The value of money is made a function of its own operation, as a directive force. The more bitcoins are worth, the more they engender an industry which builds Bitcoin.[347]

§5.873 — The Bitcoin event is a monetary Cambrian Explosion.[348] Its signature, in certain regards, is diversity. The 'coin' – in its new sense – is a generic term, to reflect this. The multiplicity of 'coins' is less a matter of amounts than of types. The re-minting of the term responds to an extraordinary proliferation in the species of comparatively cash-like money.

§5.8731 — Two basic families of alt-coins are initially distinguishable. The first consists of schismatic products from the Bitcoin main chain, generated by hard forks, in cladistic order. Bitcoin Cash (BCH) and Bitcoin SV (BSV) are the relevant lineages. Both of these coins are among the top ten cryptocurrencies by market capitalization. The second family, unified only by its contrast to the first, is far larger and more variegated, consisting of coins without Bitcoin ancestry. A number of taxonomic approaches to the principled sub-division of this alt-coin family already exist.[349]

---

[347] In the electronic wholesale markets of Shenzhen, cryptocurrency mining rigs have been added to the range of commodities on offer, alongside such comparatively recent product lines as vaping devices and drones. Here the power of incentives is starkly illustrated. This outcome was – of course – entirely unanticipated by the Bitcoin white-paper, which assumed general purpose personal computers (rather than dedicated ASICs) would be the engines of cryptocurrency mining, perhaps in perpetuity.

[348] The analogy is close enough to function as a technical description rather than a figure of speech.

[349] The classification of alt-coins initiated by Wikipedia is almost certain to prove influential, and perhaps even decisive. It grounds the most fundamental level of taxonomic order in the variation between types of consensus mechanism. Proof of work cryptocurrencies, the largest phylum (including Bitcoin and its descendents, among many others), is then sub-divided by cost-function language (SHA-256, Ethash, Scrypt, Equihash, CryptoNote, X11, Lyra2, or other).

§5.8732 — Within cryptocurrency circles, alt-coins as such are profoundly controversial. Among Bitcoin maximalists they are considered a pestilence.[350] Their existence is interpreted as a pathological side-effect of Bitcoin's emergence, and a distraction from its inevitable ascent to currency monopoly. On the other side of the ledger, strains of principled currency pluralism undoubtedly exist, even if heavily outnumbered by more opportunistic varieties of alt-coin promotion. Even if a plausible argument can be made for monetary natural monopoly, currency competition is not without a case.

§5.87321 — In respect to alt-coins, discursive controversy is not a tribunal of special importance. The market delivers a superior verdict on cryptocurrencies, with commentary – at most – as an annex. This verdict is currently mixed. The first point of note is that Bitcoin's market capitalization considerably exceeds that of all other cryptocurrencies combined.[351] In mid-2019 it was almost eight times that of Ethereum (ETH, the second ranked) and well over thirteen times that of Ripple (XRP, the third). Bitcoin, then, is evidently not merely one cryptocurrency among others. On the other hand – if not quite equally – alt-coins are nowhere close to being nothing. The latter fact is quite possibly a leading clue. That is to say, there are reasons to suspect, in regard to alt-coins, that we haven't seen anything yet.

§5.8733 — What have we seen so far? The most striking phenomenon has been a massive – and surely unprecedented – proliferation of monetary tokens. Alt-coins began to appear within a few years of the mining of Bitcoin's Genesis Block (03/01/2009).[352] Namecoin and Litecoin arrived in 2011, Peercoin in 2012. The year 2013 saw the release of Dogecoin, Gridcoin, Nxt, Primecoin, and Ripple. That July,

---

[350] A stance against alt-coins is implicit within the term Bitcoin Maximalism. Several essential ingredients of the monetary ideology make this claim uncontroversial. Bitcoin Maximalism includes at least the following commitments: (1) Any currency tends towards natural monopoly; (2) Bitcoin, as the best currency, is especially prone to exhibit this; (3) cluttering a currency with specialized traits or characteristics has no robust value, and; (4) inhibiting the ascent of Bitcoin to global monetary supremacy lacks strategic justification. Other than Bitcoin, there are only 'shit-coins' – in the argot of those most committed to the former's absolute monetary sovereignty.

[351] Cryptocurrency price movements are not only notoriously volatile, they are also highly correlated. On empirical grounds, then, or by precedent, market capitalization ratios between coins can be expected to exhibit greater stability than their absolute values. Yet this hypothesis is not perfectly neutral. Bitcoin maximalists implicitly anticipate an era of price divergence, produced by a mix of 'hyperbitcoinization' and alt-coin extinction. Neither of these trends was yet evident in late 2019. While no truly reciprocal expectation is likely – based on assumptions of general alt-coin advance relative to Bitcoin – it would be surprising if specific alt-coins had no 'maximalist' advocates. The prediction of short-term price convergence – to eventual cross-over – built into such a position is, likewise, currently undemonstrated.

A list of the top hundred coins by market capitalization can be found here: https://coinmarketcap.com/

[352] A selective list and brief description of alt-coins is provided in the apparatus. Since over a thousand alt-coins had already been released by spring 2018, an exhaustive treatment is entirely infeasible.

Mastercoin[353] – conceived as a supplementary protocol layer supported by and enhancing Bitcoin – held the first token sale (or Initial Coin Offering). Exponential growth continued into 2014, as Auroracoin, Dash, MazaCoin, Monero, NEM, NEO, PotCoin, Stellar, Titcoin, Verge, and Vertcoin, among others, deepened and broadened the product stream. Ethereum was introduced – and forked – in 2015. Tether appeared in the same year. Seven years into the crypto epoch, then, alt-coins had established themselves as a conspicuous part of the emerging monetary landscape. In the final years of the decade, the upward curve of the alt-coin economy would sharpen still further.

§5.87331 — While many alt-coins are of questionable value – and not occasionally outright scams – the flood of varied crypto tokens promoted an economic innovation of scarcely deniable importance: the ICO. An ICO – or initial coin offering – raises start-up funding through money creation. The absolute sums involved remain quite limited when compared with more conventional methods of business funding, but the trend lines have been remarkable. The socio-economic originality of the ICO is yet more remarkable.

§5.873311 — ICO revenues amounted to less than US$80 million in 2016. On a monthly basis, they peaked in September, at a little over US$21 million. The take-off year was 2017, which saw a thirty-fold increase. During the second quarter of that year, they were more than doubling each month (the pattern broke in July).[354] Over the whole year ICOs generated revenues worth over US$2.4 billion. The peak was reached – once again – in September, when US$537 million was raised. The month of June 2018 saw an extraordinary US$4.17 billion reaped by ICOs, almost entirely for EOS,[355] contributing over two-thirds of the year's total US$6.21 billion. Between spring 2016 and fall 2017, total alt-coin market cap rose from slightly under US$26 billion to over US$409 billion.

§5.873312 — An ICO is pure seigniorage. It thus restores to businesses an economic function which had been entirely alienated to the state. Unlike an IPO – the Initial Public Offering of a private company – an ICO executes a currency exchange, of a special kind.[356] The targeted ('offered') coin is characterized by its elevated virtuality. It has not yet, or actually, been in circulation prior to the ICO.

---

[353] Mastercoin was subsequently renamed Omni.

[354] Source: https://www.inc.com/john-koetsier/ico-bubble-startups-are-raising-hundreds-of-millio.html
For month-by-month 2016-2018 aggregate ICO revenue numbers, see: https://icowatchlist.com/statistics/year

[355] EOS entered the crypto space with its EOSIO blockchain protocol, as a platform for smart contracts and decentralized applications. It competes most obviously with Ethereum. The coin peaked in May 2018, with a market cap of US$15.5 billion. Almost 90% of this value had been lost by the end of the year. … The EOS.IO white paper can be found at:
https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md

[356] The difference between an IPO and an ICO is not simply qualitative. Shares, too, are money, though at a comparatively low level of intensity. (More precisely, but still vaguely, they are included in Mn where n is undetermined but > 4.)

Its value is thus discounted for risk, and for viscosity. This asymmetry on the actual-virtual axis – which is to say, in time – does the work of the ICO. Through it, the coin-releasing venture acquires actuality, bringing itself forward. Understandably, then, the ICO has been understood as an incremental advance in the formalization of an essential capitalistic function. Resourcing enterprise, through credit and then stock markets, was always an actualization mechanism. The difference lies in ever more overt and thoroughgoing monetization. Making money and making a currency communicate across a condensing continuum. Generalization of the ICO suggests eventual fusion. The end-game is for every economic project to be denominated in its own terms. At such a point, financing and currency proliferation fully converge. A new and distinct monetary epoch would not only have been initiated, but accomplished.

§5.8734 — The earliest alt-coins were Bitcoin project forks (or 'source code forks').[357] With the open-source Bitcoin protocol – and its mutant descendants – available as hereditary material, they introduced variations to optimize different parameters, by changing the balance of trade-offs between features such as transaction speed, pseudonymity, resilience, and trustlessness. In this way tokens could be flavored to different preferences, in a process of niche exploration. Within this context, Bitcoin's very substantial market dominance tends to vindicate the pattern of optimization locked into its protocol. Alternatives are comparatively unattractive. …

§5.87341 — Alt-coins, then, attend Bitcoin. They are part of what Bitcoin has brought about. In keeping with this, alt-coins have promoted themselves, typically, as 'Bitcoin 2.0' developments of the crypto space. This can mean supplementing Bitcoin, by directing blockchain-based token systems at a variety of specialized functions, and traits. It can also mean deepening the stack, by layering applications upon the Bitcoin blockchain infrastructure. Between Bitcoin and alt-coins, then, there is general – and often strong – complementarity. That synergy exceeds competition is also the market verdict. Price movements of Bitcoin and alt-coins are positively correlated. They share a fate.[358]

§5.8735 — From the mid-second decade of the new millennium, the complexity of the alt-coin ecology had grown to exceed any convenient oversight. There were already far too many coins, doing too many different things, in too many different ways, to allow accurate summary. Nothing beyond suggestive – though non-random – sampling is realistic here. Due to their remarkable diversity, Namecoin, Ripple, and Ethereum, examined briefly in series, are able to provide a rough sketch map of the alt-coin territories.

---

[357] A 'project fork' is a mutant copy. Source code is repeated, with variation. It thus tends to produce lineages analogous to those resulting from biological evolution. Abstract Darwinian dynamics are then to be expected from it. Forks of any kind are speciation events.

[358] Alt-coins are the worst way to hedge against Bitcoin.